

## I

(Beslutninger og resolutioner, henstillinger og udtalelser)

## UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR  
DATABESKYTTELSE**Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om Kommissionens meddelelse til Europa-Parlamentet og Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget med titlen — »En global metode til beskyttelse af personoplysninger i Den Europæiske Union«**

(2011/C 181/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE  
HAR —

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

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

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

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger <sup>(2)</sup>, særlig artikel 41, —

VEDTAGET FØLGENDE UDTALELSE:

**A. GENEREL DEL****1. Indledning***1.1. En første og generel vurdering*

1. Den 4. november 2010 vedtog Kommissionen en meddelelse med titlen »En global metode til beskyttelse af personoplysninger i Den Europæiske Union« (i det følgende benævnt »meddelelsen«) <sup>(3)</sup>. Meddelelsen blev sendt til høring hos Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). EDPS hilser det velkommen, at han blev hørt af Kommissionen i overensstemmelse med artikel 41 i forordning (EF) nr. 45/2001. Allerede inden vedtagelsen af meddelelsen fik EDPS mulighed for at frem-

sætte uformelle bemærkninger. Der er taget hensyn til nogle af disse bemærkninger i den endelige udgave af dokumentet.

2. Formålet med denne meddelelse er at fastlægge Kommissionens metode til modernisering af EU's retssystem med hensyn til beskyttelse af personoplysninger på alle de områder, hvor EU agerer, især på baggrund af de udfordringer, som globalisering og ny teknologi skaber <sup>(4)</sup>.
3. EDPS hilser generelt meddelelsen velkommen, da han er overbevist om, at en gennemgang af den nuværende retlige ramme for databeskyttelse er nødvendig med henblik på at sikre effektiv beskyttelse af et informations-samfund i stadig udvikling. Allerede i udtalelsen af 25. juli 2007 om gennemførelse af databeskyttelsesdirektivet <sup>(5)</sup> konkluderede han, at ændringer af direktiv 95/46/EF synes uundgåelige på længere sigt.
4. Meddelelsen udgør et vigtigt skridt hen imod en sådan lovgivningsmæssig ændring, som derefter ville være den vigtigste ændring på databeskyttelsesområdet i EU siden vedtagelsen af direktiv 95/46/EF, der generelt anses for at være grundpillen i EU's databeskyttelsespolitik (og i bredere forstand inden for EØS).
5. Meddelelsen giver de rette rammer for en målrettet revision, også fordi den generelt identificerer de væsentligste spørgsmål og udfordringer. EDPS deler Kommissionens synspunkt om, at der også vil være behov for et solidt databeskyttelsessystem i fremtiden, som baseres på den opfattelse, at eksisterende generelle principper for databeskyttelse fortsat er gældende i et samfund, der gennemgår fundamentale forandringer som følge af den hastige teknologiske udvikling og globaliseringen. Det kræver imidlertid en gennemgang af de eksisterende retlige bestemmelser.

<sup>(4)</sup> Se s. 5 i meddelelsen, første afsnit.

<sup>(5)</sup> Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 25. juli 2007 om Kommissionens meddelelse til Europa-Parlamentet og Rådet vedrørende opfølgningen på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet, EUT C 255 af 27.10.2007, s. 1.

<sup>(1)</sup> EFT L 281 af 23.11.1995, s. 31.

<sup>(2)</sup> EFT L 8 af 12.1.2001, s. 1.

<sup>(3)</sup> KOM(2010) 609 endelig.

6. Meddelelsen fremhæver med rette, at udfordringerne er enorme. EDPS deler fuldt ud dette standpunkt og understreger nødvendigheden af, at de foreslåede løsninger bør være tilsvarende ambitiøse og øge effektiviteten af beskyttelsen.

### 1.2. Formålet med udtalelsen

7. Udtalelsen vurderer de foreslåede løsninger i meddelelsen på grundlag af disse to kriterier: ambitioner og effektivitet. Den indtager generelt en positiv holdning. EDPS støtter meddelelsen, men er samtidig kritisk over for aspekter, hvor flere ambitioner efter hans opfattelse ville medføre et mere effektivt system.

8. EDPS tilstræber at bidrage med denne udtalelse til den videre udvikling af den retlige ramme for databeskyttelse. Han ser frem til Kommissionens forslag, der forventes at foreligge medio 2011, og håber, at der vil blive taget hensyn til hans forslag i ordlyden af dette forslag. Han bemærker desuden, at meddelelsen synes at udelukke visse områder, f.eks. EU-institutioners og -organers behandling af personoplysninger. Hvis Kommissionen rent faktisk skulle beslutte at udelade visse områder på dette stade — hvilket EDPS ville beklage — opfordrer han Kommissionen til at forpligte sig til at gennemføre én samlet udformning inden for en kort og nærmere angivet tidsramme.

### 1.3. Elementerne i denne udtalelse

9. Denne udtalelse står ikke alene. Den er baseret på holdninger, som EDPS og de europæiske databeskyttelsesmyndigheder tidligere har indtaget ved forskellige lejligheder. Især skal det understreges, at der i den allerede nævnte EDPS-udtalelse af 25. juli 2007 blev identificeret og udviklet nogle hovedelementer for en fremtidig ændring<sup>(6)</sup>. Den er ligeledes baseret på drøftelser med andre interessenter på området for beskyttelse af personoplysninger og privatlivets fred. Deres bidrag dannede en meget nyttig baggrund for både meddelelsen og denne udtalelse. Med hensyn hertil kan det konkluderes, at der findes et synerginiveau for, hvordan effektiviteten i databeskyttelsen forbedres.
10. Et andet vigtigt element i denne udtalelse er dokumentet med titlen »Fremtiden for privatlivets fred«, det fælles bidrag fra Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger samt

gruppen vedrørende politi og retsvæsen til den høring, som Kommissionen iværksatte i 2009 (»arbejdsgruppens dokument om fremtiden for privatlivets fred«)<sup>(7)</sup>.

11. For nylig, dvs. på en pressekonference den 15. november 2010, fremsatte EDPS sine første bemærkninger til nærværende meddelelse. Denne udtalelse uddyber de mere generelle synspunkter, som kom frem under pressekonferencen<sup>(8)</sup>.
12. Endelig anvendes der i denne udtalelse en række tidligere udtalelser fra EDPS samt af dokumenter fra Artikel 29-Gruppen vedrørende Beskyttelse af Personoplysninger. Henvisninger til disse udtalelser og dokumenter findes forskellige steder i denne udtalelse, hvor det er relevant.

## 2. Kontekst

13. Revurderingen af databeskyttelsesreglerne sker på et afgørende historisk tidspunkt. Meddelelsen beskriver sammenhængen indgående og på en overbevisende måde. På grundlag af denne beskrivelse identificerer EDPS de fire vigtigste drivkræfter, der bestemmer det miljø, hvor revurderingsprocessen finder sted.
14. Den første drivkraft er teknologisk udvikling. Dagens teknologi er ikke den samme som dengang, da direktiv 95/46/EF blev udarbejdet og vedtaget. Teknologiske fænomener såsom cloud computing, adfærdsbetinget reklame-ring, sociale netværk, opkrævning af vejafgifter og udstyr til geografisk sporing ændrede helt igennem den måde, hvorpå data behandles, og rummer enorme udfordringer for databeskyttelsen. En revurdering af de europæiske databeskyttelsesregler skal tage effektivt fat på disse udfordringer.
15. Den anden drivkraft er globaliseringen. Den gradvise afskaffelse af handelsbarrierer har givet virksomhederne en øget global dimension. Grænseoverskridende databehandling og international udveksling af oplysninger er steget voldsomt i de seneste år. Derudover er databehandling blevet allestedsnærværende i kraft af informations- og kommunikationsteknologi: internet og cloud computing har muliggjort delokaliseret behandling af store datamængder på verdensplan. Inden for de seneste ti år har

<sup>(6)</sup> Navnlig (jf. punkt 77 i denne udtalelse): Intet behov for at ændre eksisterende principper, men et klart behov for administrative ordninger, databeskyttelseslovgivningens brede anvendelsesområde bør ikke ændres, databeskyttelseslovgivningen bør give mulighed for en afbalanceret tilgang i konkrete tilfælde og bør også gøre det umuligt for databeskyttelsesmyndighederne at fastlægge prioriteter, ordningen bør i fuldt omfang gælde for anvendelsen af personoplysninger i retshåndhævelsesøjemed, selv om det kan blive nødvendigt med relevante supplerende foranstaltninger for at løse særlige problemer på dette område.

<sup>(7)</sup> Arbejdsgruppens dokument 168 ([http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf)). Hovedbudskabet heri er, at en lovændring er en god mulighed for at præcisere nogle væsentlige regler og principper (f.eks. samtykke, gennemsigtighed), indføre nogle nye principper (f.eks. »privacy by design«, ansvarlighed), styrke effektiviteten ved at modernisere ordningerne (f.eks. ved at begrænse eksisterende underretningskrav) og inddrage alle i én omfattende retlig ramme (herunder det politimæssige og strafferetlige samarbejde).

<sup>(8)</sup> Dagsordenen for konferencen findes på EDPS' websted, under: [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15\\_Press\\_conf\\_speaking\\_points\\_PHBG\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf)

man også kunnet konstatere en stigning i det internationale samarbejde mellem politi og retsvæsen for at bekæmpe terrorisme og andre former for international organiseret kriminalitet, hvilket understøttes af en enorm udveksling af oplysninger med henblik på retshåndhævelse. Alt dette nødvendiggør seriøse overvejelser om, hvordan beskyttelse af personoplysninger kan sikres effektivt i en globaliseret verden uden i væsentligt omfang at hæmme de internationale databehandlingsaktiviteter.

16. Den tredje drivkraft er Lissabontraktaten. Ikrafttrædelsen af Lissabontraktaten udgør en ny æra for databeskyttelse. EUF-traktatens artikel 16 indeholder ikke kun en individuel rettighed for den registrerede, men giver også et direkte retsgrundlag for en stærk EU-dækkende databeskyttelseslovgivning. Desuden forpligter afskaffelsen af søjlestrukturen Europa-Parlamentet og Rådet til at sørge for databeskyttelse på alle områder af EU-lovgivningen. Med andre ord muliggør den en samlet retlig ramme for databeskyttelse, som er gældende for den private sektor, den offentlige sektor i medlemsstaterne samt EU's institutioner og organer. I Stockholmprogrammet<sup>(9)</sup> anføres det konsekvent i den forbindelse, at Unionen skal sikre en samlet strategi for beskyttelse af oplysninger inden for Unionen og i dens forbindelser med andre lande.
17. Den fjerde drivkraft repræsenteres af parallelle udviklinger, som finder sted inden for de internationale organisationer. Der er forskellige igangværende drøftelser, som fokuserer på moderniseringen af de nuværende retlige instrumenter til databeskyttelse. I den sammenhæng er det væsentligt at nævne de nuværende refleksioner over den fremtidige revision af Europarådets konvention 108<sup>(10)</sup> og OECD's retningslinjer for beskyttelse af privatlivets fred<sup>(11)</sup>. En anden vigtig udvikling vedrører vedtagelsen af internationale standarder for beskyttelse af personlige oplysninger og privatlivets fred, som muligvis vil kunne føre til vedtagelsen af et bindende globalt instrument for databeskyttelse. Alle disse initiativer fortjener fuld støtte. Deres fælles mål skal være at sikre effektiv og ensartet beskyttelse i et teknologisk drevet og globaliseret samfund.

### 3. Hovedperspektiver

#### 3.1. Databeskyttelse fremmer tillid og skal understøtte andre (offentlige) interesser

18. En solid ramme for databeskyttelse er den nødvendige konsekvens af den vigtighed, som databeskyttelse tillægges i henhold til Lissabontraktaten, især i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16 i EUF-traktaten samt den tætte forbindelse til artikel 7 i charteret<sup>(12)</sup>.
19. En solid ramme for databeskyttelse tjener imidlertid også bredere offentlige og private interesser i et informations-samfund med allestedsnærværende databehandling. Databeskyttelse fremmer tilliden, og tillid er et væsentligt element til opretholdelse af vort samfunds funktionsduelighed. Det er væsentligt, at databeskyttelsesordninger konstrueres på en sådan måde, at de — så meget som muligt — aktivt støtter snarere end hæmmer andre legitime rettigheder og interesser.
20. Vigtige eksempler på andre legitime interesser er en stærk europæisk økonomi, personlig sikkerhed samt regeringers troværdighed.
21. Økonomisk udvikling i EU går hånd i hånd med indførelsen og markedsføringen af nye teknologier og tjenesteydelser. I informations-samfundet afhænger fremkomsten og en vellykket anvendelse af informations- og kommunikationsteknologier samt tjenesteydelser af tillid. Hvis folk ikke har tillid til ikt, vil disse teknologier sandsynligvis ikke få succes<sup>(13)</sup>. Og folk vil kun have tillid til ikt, hvis deres oplysninger beskyttes effektivt. Derfor skal databeskyttelse være en integreret del af teknologier og tjenesteydelser. En solid ramme for databeskyttelse fremmer den europæiske økonomi under forudsætning af, at denne ramme ikke alene er solid, men også udformet på den rigtige måde. Yderligere harmonisering inden for EU og minimering af den administrative byrde er essentiel i dette perspektiv (se afsnit 5 i denne udtalelse).
22. Der er sagt og skrevet meget i de senere år om behovet for at afbalancere privatlivets fred og den personlige sikkerhed, især hvad angår instrumenter til databehandling og -udveksling inden for det politimæssige og strafferetlige samarbejde<sup>(14)</sup>. Databeskyttelse er temmelig ofte og med urette karakteriseret som en forhindring for at opnå fuld fysisk beskyttelse af enkeltpersoner<sup>(15)</sup>, eller i det mindste som et uundgåeligt forhold, der skal respekteres af retshåndhævelsesmyndighederne. Det er imidlertid ikke hele historien. En solid ramme for databeskyttelse kan skærpe og styrke sikkerheden. På grundlag af principperne om databeskyttelse — hvis de anvendes korrekt — er de registeransvarlige forpligtet til at sikre, at oplysningerne er præcise og opdaterede, og at overflødige personlige oplysninger, som ikke er nødvendige for retshåndhævelsen, fjernes fra systemet. Det samme gælder for forpligtelsen til at gennemføre teknologiske og organisatoriske foranstaltninger til at sikre systemernes sikkerhed, f.eks.

<sup>(9)</sup> Stockholmprogrammet — Et åbent og sikkert Europa, der tjener og beskytter borgerne, EUT C 115 af 4.5.2010, s. 1, s. 10.

<sup>(10)</sup> Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention nr. 108), ETS nr. 108, 28. januar 1981.

<sup>(11)</sup> OECD's retningslinjer om beskyttelse af privatlivets fred og grænseoverskridende overførsel af personoplysninger, offentliggjort på <http://www.oecd.org>

<sup>(12)</sup> Databeskyttelsens vigtighed og forbindelsen til privatlivets fred i charteret blev understreget af EF-Domstolen i dom af 9. november 2010, forenede sager C-92/09 og C-93/09, *Schecke*, endnu ikke offentliggjort i Sml.

<sup>(13)</sup> Se udtalelse fra EDPS af 18. marts 2010 om Promoting trust in the Information Society by fostering data protection and privacy (Fremme af tillid i informationssamfundet ved at fremme databeskyttelse og privatlivets fred), EUT C 280 af 16.10.2010, s. 1, punkt 113.

<sup>(14)</sup> Se f.eks. Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om et område med frihed, sikkerhed og retfærdighed for EU's borgere, EUT C 276 af 17.9.2009, s. 8.

<sup>(15)</sup> Sikkerhed er et bredere begreb end fysisk sikkerhed, men som en illustration af de fremførte argumenter anvendes det her i dets mere begrænsede betydning.

beskyttelsessystemer mod uautoriseret videregivelse eller adgang, som er udviklet inden for databeskyttelsesområdet.

23. Overholdelse af databeskyttelsesprincipper kan desuden sikre, at retshåndhævende myndigheder opererer i henhold til retsstatslige principper, hvilket udløser tillid til deres adfærd og derfor i bredere forstand fremmer tilliden til vores samfund. Den retspraksis, der er udviklet i henhold til artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder sikrer, at politi og retsvæsen kan behandle alle oplysninger, der er relevante for deres arbejde, men ikke i ubegrænset omfang. Databeskyttelse indebærer tilsyn og kontrol (se afsnit 9 i denne udtalelse vedrørende politi og retsvæsen).
24. I demokratiske lande er regeringerne ansvarlige for alle deres aktiviteter, herunder for deres anvendelse af personlige data i forbindelse med forskellige offentlige interesser. Dette varierer fra offentliggørelsen af data på internettet med henblik på gennemsigtighed til anvendelsen af data som støtte for politikker inden for f.eks. offentlig sundhed samt transport- eller skatteområdet, eller overvågningen af enkeltpersoner med henblik på retshåndhævelse. En solid databeskyttelsesramme gør det muligt for regeringerne at opfylde deres ansvar og at være ansvarlige som led i god forvaltningsskik.

### 3.2. Konsekvenser for den retlige ramme for databeskyttelse

#### 3.2.1. Yderligere harmonisering er nødvendig

25. Meddelelsen identificerede med rette, at en af de væsentlige mangler ved den nuværende ramme er, at den overlader for meget skøn til medlemsstaterne i forbindelse med gennemførelsen af EU-bestemmelser i den nationale lovgivning. Mangel på harmonisering har en række negative konsekvenser i et informationssamfund, hvor de fysiske grænser mellem medlemsstaterne bliver mindre og mindre relevante (se afsnit 5 i denne udtalelse).

#### 3.2.2. Generelle principper om databeskyttelse er fortsat gældende

26. En første og mere formel årsag til, at de generelle principper om databeskyttelse ikke bør og ikke kan ændres er af juridisk karakter. Disse principper er fastlagt i Europarådets konvention 108, som er bindende for alle medlemsstater. Denne konvention udgør grundlaget for databeskyttelsen i EU. Desuden nævnes nogle af hovedprincipperne eksplicit i artikel 8 i Unionens charter om grundlæggende rettigheder. Ændring af disse principper ville således kræve ændring af traktaterne.
27. Det er imidlertid ikke hele historien. Der er også væsentlige årsager til ikke at ændre de generelle principper. EDPS mener afgjort, at et informationssamfund ikke kan og ikke bør fungere uden en tilstrækkelig beskyttelse af privatlivets fred og personoplysninger. Når der behandles flere oplysninger, er der også behov for bedre beskyttelse. Et informationssamfund, hvor rigelige mængder af oplysninger om alle behandles, skal baseres på et koncept med kontrol fra den enkelte, således at den pågældende får

mulighed for at fungere som enkeltperson og anvende sine friheder i et demokratisk samfund, f.eks. ytringsfriheden.

28. Desuden er det vanskeligt at forestille sig kontrol af enkeltpersoner uden forpligtelser for de registeransvarlige til at begrænse databehandlingen i overensstemmelse med principperne for nødvendighed, proportionalitet og formålsbegrænsning. På samme måde er det svært at forestille sig den enkeltes kontrol, hvis der ikke findes anerkendte rettigheder for de registrerede, f.eks. rettigheder i forbindelse med adgang til samt fejludbedring, sletning eller spærring af data.

#### 3.2.3. Grundlæggende rettigheder

29. EDPS understreger, at databeskyttelse er anerkendt som en grundlæggende rettighed. Det betyder ikke, at databeskyttelse altid skal tillægges større vægt end andre vigtige rettigheder og interesser i et demografisk samfund, men det har konsekvenser for karakteren og omfanget af den beskyttelse, der skal gives i henhold til en retlig EU-ramme, således at det sikres, at der altid tages tilstrækkelig hensyn til databeskyttelseskrav.

30. Disse hovedkonsekvenser kan defineres som følger:

- Beskyttelsen skal være effektiv. En retlig ramme skal omfatte instrumenter, der kan gøre det muligt for enkeltpersoner at udøve deres rettigheder i praksis.
- Rammen skal være stabil over en længere periode.
- Beskyttelse skal gives under alle omstændigheder og ikke afhænge af de politiske præferencer i en bestemt tidsperiode.
- Begrænsninger i forbindelse med udøvelse af rettigheden kan være nødvendige, men de skal være exceptionelle, behørigt begrundede og aldrig påvirke de essentielle elementer i selve rettigheden <sup>(16)</sup>.

EDPS anbefaler, at Kommissionen tager hensyn til disse konsekvenser, når den foreslår lovgivningsmæssige løsninger.

#### 3.2.4. Der er behov for nye retlige bestemmelser

31. Meddelelsen koncentrerer sig med rette om behovet for at styrke de retlige bestemmelser om databeskyttelse. I den sammenhæng giver det mening at minde om, at i arbejdsgruppens dokument om fremtiden for privatlivets fred <sup>(17)</sup> understregede databeskyttelsesmyndighederne behovet

<sup>(16)</sup> Se også udtalelse fra EDPS af 25. juli 2007 om Kommissionens meddelelse til Europa-Parlamentet og Rådet vedrørende opfølgningen på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet.

<sup>(17)</sup> Se fodnote 7.

for, at de forskellige aktører på databeskyttelsesområdet spiller en stærkere rolle, især de registrerede, registeransvarlige og tilsynsmyndighederne selv.

32. Der synes at være bred enighed blandt interessenter om, at mere effektive retlige bestemmelser — der tager hensyn til den teknologiske udvikling og globaliseringen — også i fremtiden er nøglen til en ambitiøs og effektiv beskyttelse. Som allerede anført i punkt 7, er dette kriterierne for den vurdering, som EDPS foretager af alle foreslåede løsninger.

### 3.2.5. Omfang som en ufravigelig betingelse

33. Som præciseret i meddelelsen gælder direktiv 95/46/EF for alle databehandlingsaktiviteter i medlemsstaterne i såvel den offentlige som i den private sektor med undtagelse af aktiviteter, der er omfattet af tidligere fællesskabslovgivning<sup>(18)</sup>. Mens denne undtagelse var nødvendig i henhold til den tidligere traktat, er dette ikke længere tilfældet efter ikrafttrædelsen af Lissabontraktaten. Desuden er undtagelsen i strid med — teksten og under alle omstændigheder ånden i — EUF-traktatens artikel 16.

34. Ifølge EDPS skal ét samlet retligt instrument for databeskyttelse, herunder politisamarbejde og retligt samarbejde i kriminalsager, ses som en af de væsentlige forbedringer, som en ny retlig ramme kan medføre. Dette er en ufravigelig betingelse for effektiv databeskyttelse i fremtiden.

35. EDPS fremhæver følgende argumenter til støtte for dette udsagn:

— Sondringen mellem aktiviteter i den private sektor og retshåndhævelsessektoren er diffus. Privatretlige organer kan behandle oplysninger, der i sidste ende anvendes til retshåndhævelsesformål (eksempelvis: PNR-data<sup>(19)</sup>), mens de i andre tilfælde skal opbevare oplysninger til retshåndhævelsesformål (eksempelvis: Datalagringsdirektivet<sup>(20)</sup>).

— Der er ikke nogen fundamental forskel mellem politi- og retsmyndigheder og andre myndigheder, som forestår retshåndhævelse (told- og skattemyndigheder, bedragerimyndigheder samt immigrationsmyndigheder) i henhold til direktiv 95/46/EF.

<sup>(18)</sup> Denne udtalelse vil hovedsagelig fokusere på den tidligere 3. søjle (politisamarbejde og retligt samarbejde i kriminalsager), da den tidligere 2. søjle ikke kun er et mere kompliceret område i EU-lovgivningen (anerkendt ved EUF-traktatens artikel 16 og artikel 39 EU), men også i mindre grad er relevant for databehandling.

<sup>(19)</sup> Se f.eks. meddelelse fra Kommissionen om den globale tilgang til overførsel af passageroplysninger (PNR) til tredjelande, KOM(2010) 492 endelig.

<sup>(20)</sup> Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT L 105 af 13.4.2006, s. 54).

— Som det beskrives udførligt i meddelelsen, er det retlige instrument for databeskyttelse, der på nuværende tidspunkt gælder for politi- og retsmyndigheder (rammeafgørelse 2008/977/RIA<sup>(21)</sup>), utilstrækkeligt.

— De fleste medlemsstater har gennemført direktiv 95/46/EF og konvention 108 i deres nationale lovgivninger, hvilket betyder, at de er gældende for deres politi- og retsmyndigheder.

36. Inddragelse af politi og retsvæsen i det generelle retlige instrument ville ikke kun tilvejebringe flere garantier til borgerne, men også gøre opgaven lettere for politimyndighederne. At skulle anvende forskellige regelsæt er besværligt, unødigt tidskrævende og står i vejen for internationalt samarbejde (se også afsnit 9 i denne udtalelse). Dette er også et argument for at medtage de nationale sikkerhedstjenesters databehandlingsaktiviteter, for så vidt dette er muligt i overensstemmelse med EU-lovgivningens aktuelle situation.

### 3.2.6. Teknologisk neutralitet

37. Perioden siden vedtagelsen af direktiv 95/46/EF i 1995 kan karakteriseres som teknologisk turbulent. Ny teknologisk udvikling og nyt udstyr introduceres med hyppige mellemrum. I mange tilfælde har dette medført grundlæggende ændringer af den måde, som personoplysninger behandles på. Informationssamfundet kan ikke længere anses som et parallelt samfund, hvor enkeltpersoner kan deltage på frivillig basis, men er blevet en integreret del af vores dagligdag. Bare som et eksempel knytter et »tingenes internet«<sup>(22)</sup> forbindelse mellem fysiske ting og onlineoplysninger i relation hertil.

38. Teknologien vil blive yderligere udviklet. Dette har konsekvenser for den nye retlige ramme. Den skal være effektiv i en længere årrække, og samtidig må den ikke hæmme yderligere teknologisk udvikling. Det kræver, at de juridiske foranstaltninger er teknologineutrale. Rammen skal imidlertid også skabe større retssikkerhed for virksomheder og enkeltpersoner. De skal forstå, hvad der forventes af dem og være i stand til at udøve deres rettigheder. Det kræver, at de juridiske foranstaltninger er præcise.

39. Ifølge EDPS skal et generelt retligt instrument om databeskyttelse så vidt muligt formuleres på en teknologineutral måde. Dette indebærer, at de forskellige aktørers rettigheder og forpligtelser skal formuleres på en generel og neutral måde, således at de i princippet fortsat er gyldige og har retskraft, uafhængigt af den teknologi, der måtte vælges til behandling af personoplysninger. Der er intet andet valg set i lyset af dagens hurtige teknologiske udvikling. EDPS foreslår indførelsen af

<sup>(21)</sup> Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i straffesager, EUT L 350 af 30.12.2008, s. 60.

<sup>(22)</sup> Som defineret på »Tingenes internet« — en EU-handlingsplan, KOM(2009) 278 endelig.

nye »teknologineutrale« rettigheder på toppen af de eksisterende principper om databeskyttelse, hvilket kunne få væsentlig betydning i et elektronisk samfund under hastig forandring (se især afsnit 6 og 7).

### 3.2.7. Lang sigt: Retssikkerhed i en længere periode

40. Direktiv 95/46/EF har været det centrale element inden for databeskyttelse i EU i de seneste 15 år. Det blev implementeret i medlemsstaternes lovgivninger og anvendt af forskellige aktører. I gennem årene har man udnyttet praktiske erfaringer og yderligere retningslinjer fra Kommissionen, databeskyttelsesmyndighederne (på nationalt niveau og inden for rammerne af Artikel 29-Gruppen) samt nationale og europæiske domstole.

41. Det er vigtigt at pointere, at denne udvikling har brug for tid — især da vi har at gøre med en generel ramme, der har indvirkning på en grundlæggende rettighed — og at tiden skal bruges til at skabe retssikkerhed og stabilitet. Der skal udfærdiges et nyt generelt retligt instrument med en ambition om, at det vil kunne skabe retssikkerhed og stabilitet i en længere periode, idet man skal huske på, at det er meget vanskeligt at forudsige, hvordan teknologien og globaliseringen udvikler sig fremover. Under alle omstændigheder støtter EDPS fuldt ud målet om at skabe retssikkerhed i en længere periode, der er sammenlignelig med perspektivet for direktiv 95/46/EF. Kort sagt betyder det, at når teknologien udvikler sig hurtigt, skal lovgivningen være stabil.

### 3.2.8. Kort sigt: Gøre bedre brug af eksisterende instrumenter

42. På kort sigt er det absolut nødvendigt at sikre effektiviteten af eksisterende løbbestemmelser, hvilket i første omgang skal ske ved at koncentrere sig om håndhævelse, på nationalt og EU-niveau (se afsnit 11 i denne udtalelse).

## B. ELEMENTER I EN NY RAMME

### 4. Samlet tilgang

43. EDPS støtter fuldt ud én samlet tilgang til databeskyttelse, hvilket ikke blot er titlen, men også udgangspunktet for meddelelsen, og som nødvendigvis omfatter en udvidelse af de generelle databeskyttelsesregler til politisamarbejde og retligt samarbejde i kriminalsager<sup>(23)</sup>.

44. Han bemærker imidlertid også, at Kommissionen ikke påtænker at medtage alle databehandlingsaktiviteter i dette generelle retlige instrument. Især databehandling, der udføres af EU's institutioner, organer, kontorer og agenturer, omfattes ikke heraf. Kommissionen angiver kun, at den »vil vurdere behovet for at tilpasse andre retlige instrumenter til den nye generelle retlige ramme for databeskyttelse«.

45. EDPS har en klar præference for at indsætte databehandling på EU-niveau i den generelle retlige ramme. Han minder om, at dette var den oprindelige intention med den tidligere artikel 286 i traktaten om oprettelse af Det Europæiske Fællesskab, hvor databeskyttelse blev nævnt for første gang på traktatniveau. Af artikel 286 fremgår, at retlige instrumenter om behandling af personoplysninger også ville gælde for institutionerne. Mere væsentligt undgår en retsakt risikoen for afvigelser mellem bestemmelser og ville være bedst egnet til dataoverførsel mellem EU og de offentlige og private enheder i medlemsstaterne. Dermed ville man efter ændring af direktiv 95/46/EF undgå risikoen for, at der ikke længere er nogen politisk interesse i at ændre forordning (EF) nr. 45/2001 eller at give denne ændring tilstrækkelig prioritering med henblik på at undgå afvigelser i forbindelse med ikrafttrædelsesdatoer.

46. EDPS opfordrer kraftigt Kommissionen — i tilfælde af, at den skulle konkludere, at indsættelsen af databehandling på EU-niveau i det generelle retlige instrument ikke ville være mulig — til at forpligte sig til at foreslå en vedtagelse af forordning (EF) nr. 45/2001 (ikke til at »vurdere behovet«) inden for den kortest mulige tidsramme og helst inden udgangen af 2011.

47. Det er ligeledes vigtigt, at Kommissionen sikrer, at andre områder ikke lades i stikken, herunder især:

— Databeskyttelse i den fælles udenrigs- og sikkerhedspolitik på grundlag af EUF-traktatens artikel 39<sup>(24)</sup>.

— Sektorspecifikke databeskyttelseordninger for EU-organer såsom Europol, Eurojust og for store informationssystemer, for så vidt de skal tilpasses til det nye retlige instrument.

— E-direktivet om privatlivets fred 2002/58/EF, for så vidt det skal tilpasses til det nye retlige instrument.

48. Endelig kan og sandsynligvis skal et generelt retligt instrument for databeskyttelse suppleres af yderligere sektorale og specifikke bestemmelser, f.eks. hvad angår samarbejdet mellem politi og retsvæsen, men også på andre områder<sup>(25)</sup>. Hvor det er nødvendigt og i overensstemmelse med nærhedsprincippet, skal disse yderligere bestemmelser vedtages på EU-niveau. Medlemsstater kan fastsætte yderligere regler på specifikke områder, hvor dette er berettiget (se 5.2).

<sup>(24)</sup> Se også udtalelse fra EDPS af 24. november 2010 om Kommissionens meddelelse til Europa-Parlamentet og Rådet vedrørende EU's terrorbekæmpelsespolitik: vigtigste resultater og fremtidige udfordringer, punkt 31.

<sup>(25)</sup> Se også arbejdsgruppens dokument om fremtiden for privatlivets fred (fodnote 7), punkt 18-21.

<sup>(23)</sup> Se s. 14 i meddelelsen og afsnit 3.2.5 i denne udtalelse.

## 5. Yderligere harmonisering og forenkling

### 5.1. Behovet for harmonisering

49. Harmonisering er yderst vigtigt for EU's databeskyttelseslovgivning. Meddelelsen fremhævede med rette, at databeskyttelse har en stærk indre markeds dimension, da den skal sikre det frie flow af personoplysninger mellem medlemsstaterne inden for det indre marked. Harmoniseringsniveauet i henhold til det nuværende direktiv er imidlertid blevet bedømt til at være mindre end tilfredsstillende. Meddelelsen anerkender, at dette er en af interessenternes tilbagevendende hovedbekymringer. Interessenterne betoner navnlig behovet for at øge retssikkerheden, reducere den administrative byrde og sikre lige vilkår for økonomiske operatører. Som Kommissionen med rette anfører, er dette især tilfældet for registeransvarlige, der er etableret i flere medlemsstater og forpligtet til at overholde de (muligvis divergerende) krav i de nationale databeskyttelseslove <sup>(26)</sup>.

50. Harmonisering er ikke alene vigtig for det indre marked, men også med henblik på at sikre tilstrækkelig databeskyttelse. EUF-traktatens artikel 16 foreskriver, at »enhver« har ret til beskyttelse af personoplysninger, som vedrører dem. Med henblik på at sikre effektiv overholdelse af denne rettighed skal der garanteres et tilsvarende beskyttelsesniveau i hele EU. Arbejdsgruppens dokument om fremtiden for privatlivets fred fremhævede, at adskillige bestemmelser vedrørende de registreredes rettigheder ikke er blevet gennemført eller fortolket ens i alle medlemsstater <sup>(27)</sup>. I en globaliseret og indbyrdes forbundet verden kan disse forskelle underminere eller begrænse beskyttelsen af enkeltpersoner.

51. EDPS er af den opfattelse, at yderligere og bedre harmonisering er et af hovedmålene for denne revurderingsproces. EDPS hilser Kommissionens tilsagn velkommen om at undersøge midlerne til at opnå yderligere harmonisering af databeskyttelsen på EU-niveau. Han konstaterer dog med nogen overraskelse, at meddelelsen ikke fremkommer med nogen konkrete muligheder på dette stadi. Han giver derfor udtryk for et par områder, hvor der er et presserende behov for større konvergens (se 5.3). Yderligere harmonisering på disse områder skal ikke alene opnås ved at reducere manøvreremargenen for den nationale lovgivning, men også ved at forhindre medlemsstaters ukorrekte gennemførelse (se også afsnit 11) og sikre en mere ensartet og samordnet håndhævelse (se også afsnit 10).

### 5.2. Reduktion af manøvreremargenen ved gennemførelsen af direktivet

52. Direktivet indeholder en række bestemmelser, der er bredt formuleret, og som derfor efterlader betydelig plads til

divergerende gennemførelse. Betragtning 9 i direktivet bekræfter eksplicit, at medlemsstaterne får en vis manøvreremargen, og at der inden for denne margen kan opstå forskelle i gennemførelsen af direktivet. Flere bestemmelser er blevet gennemført forskelligt af medlemsstaterne, herunder nogle afgørende bestemmelser <sup>(28)</sup>. Situationen er ikke tilfredsstillende, og der skal sigtes mod større konvergens.

53. Dette betyder ikke, at forskellighed ligefrem skal udelukkes. På visse områder kan der være behov for fleksibilitet med henblik på at bevare berettigede specificiteter, væsentlige offentlige interesser eller medlemsstaternes institutionelle autonomi. Ifølge EDPS skal råderummet for divergenser mellem medlemsstaterne begrænses, navnlig til følgende specifikke situationer:

— Ytringsfrihed: I henhold til den nuværende ramme (artikel 9) kan medlemsstaterne fastsætte undtagelser og afvigelser i relation til behandlingen af data, der finder sted i journalistisk øjemed eller med henblik på kunstnerisk eller litterær virksomhed. Denne fleksibilitet synes at være på sin plads, idet den naturligvis er underlagt begrænsningerne i charteret og den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (EMRK) i lyset af de forskellige traditioner og kulturelle forskelle, der kan være på dette område på tværs af medlemsstaterne. Dette vil imidlertid ikke stå i vejen for en eventuel opdatering af den nuværende artikel 9 på baggrund af udviklingen på internettet.

— Specifikke offentlige interesser: I henhold til den nuværende ramme (artikel 13) kan medlemsstaterne vedtage lovgivningsmæssige foranstaltninger for at begrænse omfanget af forpligtelserne og rettighederne, hvis en sådan begrænsning udgør en nødvendig foranstaltning for at sikre væsentlige offentlige interesser, f.eks. national sikkerhed, forsvar, offentlig sikkerhed osv. At denne kompetence ligger hos medlemsstaterne er fortsat berettiget. Hvor det er muligt, skal fortolkningen af undtagelserne dog harmoniseres yderligere (se afsnit 9.1). Desuden forekommer det nuværende omfang af undtagelsen til artikel 6, stk. 1, at være urimeligt omfattende.

— Klagemuligheder, sanktioner og administrative procedurer: En europæisk ramme skal fastlægge de vigtigste betingelser, men i overensstemmelse med EU-lovgivningens aktuelle situation skal fastlæggelse af sanktioner, klagemuligheder, procedureregler og tilsynsmetoder, hvor det er relevant på nationalt niveau, overlades til medlemsstaterne.

<sup>(26)</sup> Meddelelse, s. 10.

<sup>(27)</sup> Se arbejdsgruppens dokument om fremtiden for privatlivets fred (fodnote 7), punkt 70. Dokumentet henviser navnlig til ansvarsbestemmelser og muligheden for at kræve erstatning for immateriel skade.

<sup>(28)</sup> Der findes også forskellige tiltag for så vidt angår manuelle data.

### 5.3. Områder til yderligere harmonisering

54. *Definitioner* (artikel 2 i direktiv 95/46/EF). Definitioner er grundpiller i retssystemet og skal fortolkes ens i alle medlemsstater uden nogen gennemførelsesmargen. Der er opstået forskelle i henhold til den nuværende ramme, f.eks. hvad angår begrebet registeransvarlig<sup>(29)</sup>. EDPS foreslår at tilføje yderligere punkter på den eksisterende liste i artikel 2 med henblik på at opnå større retssikkerhed, f.eks. anonyme data, pseudonyme data, juridiske data, dataoverførsel og databeskyttelsesansvarlig.
55. *Lovlig behandling af personoplysninger* (artikel 5). Det nye retlige instrument skal være så præcist som muligt med hensyn til de kernelementer, der bestemmer den lovlige behandling af personoplysninger. Artikel 5 i direktivet (samt betragtning 9), som giver medlemsstaterne mandat til mere præcist at fastlægge betingelserne for, hvornår denne behandling er lovlig, er således måske ikke længere nødvendig i en fremtidig ramme.
56. *Grunde til databehandling* (artikel 7 og 8). Definitionen af betingelserne for databehandling er et væsentligt element i enhver databeskyttelseslovgivning. Medlemsstater må ikke få lov til at indføre yderligere eller ændrede grunde til behandling eller udelukke nogle. Muligheden for afvigelser skal udelukkes eller begrænses (navnlig i forbindelse med følsomme data<sup>(30)</sup>). I et nyt retligt instrument skal grundene til databehandling være klart formuleret, hvorved skønsbeføjelsen reduceres ved gennemførelsen eller håndhævelsen. Især kan der være behov for at specificere begrebet samtykke yderligere (se afsnit 6.5). Endvidere åbner den grund, der er baseret på den registeransvarliges berettigede interesse (artikel 7, litra f), mulighed for vidt forskellige fortolkninger på grund af dens fleksible karakter. Yderligere præcisering er nødvendig. En anden bestemmelse, der eventuelt skal specificeres, er artikel 8, stk. 2, litra b), der tillader behandling af følsomme data, som er nødvendige med henblik på at udføre den registeransvarliges forpligtelser og særlige rettigheder på det arbejdsretlige område<sup>(31)</sup>.
57. *Den registreredes rettigheder* (artikel 10-15). Dette er et af de områder, hvor ikke alle elementer af direktivet er blevet konsekvent gennemført og fortolket af medlemsstaterne. De registreredes rettigheder er et centralt element for en effektiv databeskyttelse. Som en konsekvens heraf skal råderummet være væsentligt reduceret. EDPS anbefaler, at de oplysninger, som den registeransvarlige videregiver til de registrerede, bør være ens i hele EU.
58. *Internationale overførsler* (artikel 25-26). Det er et område, som har givet anledning til omfattende kritik på grund af manglen på en fælles praksis inden for EU. Interessenter kritiserede, at Kommissionens afgørelser om tilstrækkelighed fortolkes og gennemføres meget forskelligt af medlemsstaterne. Bindende virksomhedsregler er et andet element, hvor EDPS anbefaler yderligere harmonisering (se afsnit 9).
59. *Nationale databeskyttelsesmyndigheder* (artikel 28). Nationale databeskyttelsesmyndigheder er underlagt vidt forskellige regler i de 27 medlemsstater, især hvad angår deres status, ressourcer og beføjelser. Artikel 28 har delvist bidraget til denne forskellighed på grund af manglen på præcision<sup>(32)</sup> og skal specificeres yderligere i overensstemmelse med EF-Domstolens dom i sag C-518/07<sup>(33)</sup> (se desuden afsnit 10).

### 5.4. Forenkling af underretningssystemet

60. *Underretningskrav* (artikel 18-21 i direktiv 95/46/EF) er et andet område, hvor medlemsstaterne indtil nu har fået væsentlig frihed. Meddelelsen anerkender med rette, at et harmoniseret system ville reducere omkostningerne samt den administrative byrde for de registeransvarlige<sup>(34)</sup>.
61. Det er et område, hvor forenkling skal være det primære mål. Revurderingen af databeskyttelsesrammerne er en unik mulighed for yderligere at forenkle og/eller reducere omfanget af de nuværende underretningskrav. Meddelelsen anerkender, at der er generel enighed blandt interessenterne om, at det eksisterende underretningssystem er temmelig besværligt og ikke i sig selv giver merværdi til beskyttelsen af personoplysninger<sup>(35)</sup>. EDPS hilser derfor Kommissionens forpligtelse til at undersøge forskellige muligheder for forenkling af det nuværende underretningssystem velkommen.
62. Efter hans mening må udgangspunktet for denne forenkling være et skifte fra et system, hvor underretning er reglen, medmindre andet er bestemt (dvs. »fritagelsesordning«), til et mere målrettet system. Fritagelsesordningen viste sig at være ineffektiv, da den blev gennemført på en inkonsekvent måde på tværs af medlemsstaterne<sup>(36)</sup>. EDPS anbefaler, at man overvejer følgende alternativer:

<sup>(29)</sup> Arbejdsgruppens dokument om fremtiden for privatlivets fred, punkt 87.

<sup>(33)</sup> Sag C-518/07, *Kommissionen mod Tyskland*, endnu ikke offentliggjort i ECR.

<sup>(34)</sup> Se fodnote 26.

<sup>(35)</sup> Se fodnote 26.

<sup>(36)</sup> Artikel 29-Gruppens rapport om forpligtelsen til at underrette de nationale tilsynsmyndigheder, den bedste anvendelse af undtagelser og forenklinger og de databeskyttelsesansvarliges rolle i EU, arbejdsgruppens dokument 106, 2005, s. 7.

<sup>(29)</sup> Se Artikel 29-Gruppens udtalelse 1/2010 om koncepterne for den »registeransvarlige« og »registerføreren« (arbejdsgruppens dokument 169).

<sup>(30)</sup> Artikel 8, stk. 4 og 5, tillader på nuværende tidspunkt medlemsstaterne at fastsætte yderligere afvigelser for så vidt angår følsomme data.

<sup>(31)</sup> Se i den sammenhæng Kommissionens første beretning om gennemførelsen af databeskyttelsesdirektivet, s. 14.



- Begrænse underrettningsforpligtelsen til visse former for behandlingskørsler, som indebærer særlige risici (disse underretninger kunne udløse yderligere skridt, f.eks. forudgående kontrol).
- En simpel registreringsforpligtelse for de registransvarlige til at registrere (i modsætning til omfattende registrering af alle databehandlingsoperationer).

Derudover kunne der indføres en fælleseuropæisk standardformular til underretningen for at sikre harmoniserede metoder med hensyn til de ønskede oplysninger.

63. Revurderingen af det nuværende underretningssystem skal ikke være til hinder for at forbedre forudgående kontrolforpligtelser for visse behandlingsforpligtelser, der kan indebære særlige risici (f.eks. store informationssystemer). EDPS ville foretrække indsættelsen i det nye retlige instrument af en ikkeudtømmende liste over tilfælde, hvor en sådan forudgående kontrol er nødvendig. Forordning (EF) nr. 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne udgør en nyttig model til dette formål <sup>(37)</sup>.

#### 5.5. En forordning, ikke et direktiv

64. Endelig finder EDPS, at denne revurderingsproces også er en mulighed for at genoverveje den form, som det retlige instrument for databeskyttelse skal have. En forordning, et enkelt instrument, der er umiddelbart gældende i medlemsstaterne, er den mest effektive måde at beskytte den grundlæggende ret til databeskyttelse og til at skabe et indre marked, hvor personoplysninger frit kan overføres, og hvor beskyttelsesniveauet er tilsvarende uafhængigt af det land eller den sektor, hvor dataene behandles.
65. En forordning ville reducere råderummet for modstridende fortolkninger og for uberettigede forskelle i gennemførelsen og anvendelsen af loven. Desuden ville den reducere vigtigheden af at fastlægge den lov, der gælder for behandlingsoperationer inden for EU, hvilket er et af de mest kontroversielle aspekter ved det nuværende system (se afsnit 9).
66. På databeskyttelsesområdet er en forordning så meget desto mere berettiget, fordi
- EUR-traktatens artikel 16 har opgraderet retten til beskyttelse af personoplysninger til traktatniveau og forudser — eller giver endog mandat til — et ensartet beskyttelsesniveau for den enkelte inden for EU.
  - Databehandling finder sted i et elektronisk samfund, hvor indre grænser mellem medlemsstaterne er blevet mindre relevante.

67. Valget af en forordning som et generelt instrument giver mulighed for, hvor det er nødvendigt, bestemmelser, der er direkte rettet mod medlemsstaterne, hvor fleksibilitet er påkrævet. Det påvirker heller ikke medlemsstaternes beføjelse til at vedtage yderligere regler for databeskyttelse, hvor det er nødvendigt, i overensstemmelse med EU-lovgivningen.

## 6. Styrkelse af enkeltpersoners rettigheder

### 6.1. Behovet for at styrke rettighederne

68. EDPS støtter fuldt ud meddelelsen, hvori der foreslås en styrkelse af den enkeltes rettigheder, da de eksisterende retlige instrumenter ikke helt giver den effektive beskyttelse, der er nødvendig i en stadigt mere kompleks digitaliseret verden.
69. På den ene side medfører udviklingen af en digitaliseret verden en stærk vækst i indsamlingen, anvendelsen og yderligere overførsel af personoplysninger på en ekstrem kompleks og ikkegennemsigtig måde. Enkeltpersoner er ofte ikke opmærksomme på eller forstår ikke, hvordan dette sker, hvem der indsamler deres data, eller hvordan der udøves kontrol hermed. Dette fænomen illustreres ved den overvågning, som udbydere af annoncenetværk udfører ved hjælp af cookies og andet udstyr til at overvåge individuelle brugeres adfærd, når de surfer på internettet, for at kunne sende dem målrettede annoncer. Når brugerne besøger websteder, forventer de ikke, at en ikke synlig tredjepart registrerer disse besøg og opbygger brugerprofiler, der er baseret på oplysninger, som afslører deres livsstil, eller hvad de kan eller ikke kan lide.
70. På den anden side stimulerer udviklingen individuelle brugeres proaktive deling af deres personoplysninger, f.eks. på sociale netværk. Stadigt flere unge indgår i et socialt netværk og interagerer med deres jævnaldrende. Det er tvivlsomt, hvorvidt (unge) mennesker er klar over rækkevidden af deres videregivelse af personoplysninger og de langsigtede virkninger af deres handlinger.

### 6.2. Større gennemsigtighed

71. Gennemsigtighed har afgørende betydning i enhver databeskyttelsesordning, ikke alle på grund af dens iboende værdi, men også fordi den muliggør udøvelse af andre databeskyttelsesprincipper. Kun hvis individuelle brugere har kendskab til databehandlingsprocessen, vil de kunne udøve deres rettigheder.
72. Adskillige bestemmelser i direktiv 95/46/EF omhandler gennemsigtighed. Artikel 10 og 11 indeholder en forpligtelse til at give oplysninger til individuelle brugere om indsamlingen af deres personoplysninger. Derudover anerkender artikel 12 retten til en kopi af ens egne personoplysninger i letforståelig form (ret til indsigt). Artikel 15 anerkender retten til indsigt i den logik, der ligger bag edb-behandlingen af afgørelser, der har retsvirkning. Sidst men ikke mindst indebærer artikel 6.1, litra a), hvori der kræves loyal behandling af personoplysninger, også et krav om gennemsigtighed. Personoplysninger kan ikke behandles af skjulte eller hemmelige årsager.

<sup>(37)</sup> Se artikel 27 i forordningen, EFT L 8 af 12.1.2001, s. 1.

73. Personoplysninger kan ikke behandles af skjulte eller hemmelige årsager. Meddelelsen foreslår at tilføje et generelt princip om gennemsigtighed. Som en reaktion på dette forslag understreger EDPS, at begrebet gennemsigtighed allerede er en integreret del af den nuværende retlige ramme for databeskyttelse, omend på en implicit måde. Dette kan udledes af de forskellige bestemmelser vedrørende gennemsigtighed, som nævnt i det foregående punkt. EDPS mener, at det vil kunne betyde merværdi at inkorporere et *eksplicit* princip om gennemsigtighed, hvad enten det har eller ikke har forbindelse til den eksisterende bestemmelse om loyal behandling af personoplysninger. Dette ville øge retssikkerheden og også bekræfte, at en registeransvarlig under alle omstændigheder skal behandle data på en gennemsigtig måde, ikke kun på forlangende, eller hvis en specifik retsforordning kræver det.
74. Men det er måske mere vigtigt at styrke de eksisterende bestemmelser vedrørende gennemsigtighed, f.eks. artikel 10 og 11 i direktiv 95/46/EF. Disse bestemmelser angiver de informationselementer, der skal foreligge, men er ikke præcise med hensyn til enkelthederne. Mere konkret foreslår EDPS en styrkelse af de eksisterende bestemmelser i form af:
- Et krav om, at den registeransvarlige skal give oplysninger om databehandling på en måde, som er nemt tilgængelig og letforståelig samt i et klart og forståeligt sprog<sup>(38)</sup>. Oplysningerne skal være klare, tydelige og iøjnefaldende. Bestemmelsen kunne også omfatte en forpligtelse til at sikre nem forståelse af oplysningerne. Denne forpligtelse ville give ulovlige databeskyttelsespolitikker, der er uigennemsigtige eller vanskelige at forstå.
  - Et krav om at formidle oplysningerne nemt og direkte til de registrerede. Oplysningerne skal ligeledes være permanent tilgængelige og ikke efter en meget kort periode forsvinde fra et elektronisk medium. Dette ville hjælpe brugerne med at opbevare og reproducere oplysninger i fremtiden, der muliggør yderligere adgang.
- 6.3. *Støtte til en rapporteringsforpligtelse med hensyn til sikkerhedsbrud*
75. EDPS bifalder indførelsen af en bestemmelse vedrørende underretning om brud på datasikkerheden i det generelle instrument, hvilket udvider den forpligtelse, der var indsat i det reviderede e-direktiv om privatlivets fred, for visse udbydere til alle registeransvarlige som foreslået i meddelelsen. I henhold til det reviderede e-direktiv om privatlivets fred gælder forpligtelsen kun for udbydere af elektroniske kommunikationstjenester (udbydere af telefonitjenester (herunder VoIP) og internetadgang). Andre registeransvarlige er ikke omfattet af denne forpligtelse. De grunde, der berettiger forpligtelsen, gælder fuldt ud for alle andre registeransvarlige end udbydere af elektroniske kommunikationstjenester.
76. Underretning om brud på sikkerheden tjener forskellige formål og mål. Den mest åbenlyse, der er fremhævet i meddelelsen, er at fungere som et informationsredskab til at gøre enkeltpersoner opmærksom på de risici, de står over for, hvis deres personoplysninger kompromiteres. Dette kan hjælpe dem til at tage de nødvendige forholdsregler for at afværge sådanne risici. F.eks. vil enkeltpersoner, når de informeres om brud på sikkerheden, som påvirker deres finansielle oplysninger, bl.a. kunne ændre passwords eller ophæve deres konti. Derudover bidrager underretning om brud på sikkerheden til den effektive anvendelse af andre principper og forpligtelser i direktivet. Eksempelvis tilskynder krav til underretning om brud på sikkerheden de registeransvarlige til at gennemføre mere effektive sikkerhedsforanstaltninger for at forhindre overtrædelser af reglerne. Sikkerhedsbrud er også et redskab til at styrke de registeransvarliges ansvar og navnlig øge ansvarligheden (se afsnit 7). Endelig er det et håndhævelsesredskab for databeskyttelsesmyndighederne. Underretning om brud på sikkerheden til databeskyttelsesmyndighederne kan foranledige en undersøgelse af en registeransvarligs generelle praksisser.
77. De særlige regler om sikkerhedsbrud i det reviderede e-direktiv blev drøftet intenst under den parlamentariske fase af lovforberedelsen, der gik forud for vedtagelsen af e-direktivet om privatlivets fred. Under disse drøftelser blev der taget hensyn til udtalelserne fra Artikel 29-Gruppen og EDPS sammen med synspunkter fra andre interessenter. Reglerne afspejler synspunkter fra forskellige interessenter. De repræsenterer en ligevægt mellem interessenteres interesser: Mens de kriterier, der udløser underretningsforpligtelsen, i princippet er tilstrækkelige til at beskytte enkeltpersoner, gør de dette uden at pålægge nogle overdrevent besværlige krav, der ikke er brugbare.
- 6.4. *Styrkelse af regler om samtykke*
78. Artikel 7 i databeskyttelsesdirektivet oplister seks retsgrundlag for behandling af personoplysninger. Samtykke fra den enkelte er det ene. En registeransvarlig kan behandle personoplysninger i det omfang, at enkeltpersoner har afgivet informeret samtykke til at have deres data indsamlet og yderligere behandlet.
79. I praksis har brugerne ofte begrænset kontrol i forhold til deres data, navnlig i teknologiske samfund. En af de metoder, der undertiden anvendes, er stiltiende samtykke, hvilket er samtykke, der er blevet udledt. Det kan udledes af den enkeltes handling (f.eks. anses en handling, der består i at bruge et websted, for at give samtykke til at

<sup>(38)</sup> Se meddelelse, s. 6.

registrere brugerens data til markedsføringsformål). Det kan også udledes af tavshed eller manglende handling (at undlade at afklikke en afkrydset boks anses for at være samtykke).

80. I henhold til direktivet skal et samtykke for at være gyldigt være informeret, frivilligt givet og udtrykkeligt. Det skal være en informeret angivelse af enkeltpersonens ønsker, hvormed han underskriver en aftale, der tillader behandling af personoplysninger vedrørende ham. Den måde, hvorpå samtykke gives, skal være utvetydig.
81. Samtykke, der er udledt ved et søgsmål og nærmere bestemt af tavshed eller manglende handling er ofte ikke et utvetydigt samtykke. Det er imidlertid ikke altid klart, hvad der udgør ægte, utvetydigt samtykke. Nogle registeransvarlige udnytter denne usikkerhed ved at påberåbe sig metoder, som ikke er egnede til at give ægte, utvetydigt samtykke.
82. I lyset af ovenstående støtter EDPS Kommissionen med hensyn til behovet for at præcisere grænserne for samtykke og at sikre, at kun samtykke, der er fortolket på en pålidelig måde, skal opfattes som sådan. I den sammenhæng foreslår EDPS som følger<sup>(39)</sup>:
- Det bør overvejes at udvide de situationer, hvor udtrykkeligt samtykke er påkrævet, som i øjeblikket er begrænset til følsomme data.
  - Vedtage yderligere regler for samtykke i online-miljøet.
  - Vedtage yderligere regler for samtykke til at behandle data til sekundære formål (dvs., at behandlingen er underordnet i forhold til hovedbehandlingen eller ikke indlysende).
  - I et yderligere lovgivningsinstrument, hvad enten det er eller ikke er vedtaget af Kommissionen i henhold til EUF-traktatens artikel 290, fastsættes den type samtykke, der er nødvendig, eksempelvis med henblik på nærmere angivelse af niveauet for samtykke til behandling af data fra RFID-etiketter på forbrugsvarer eller til andre specifikke teknikker.

#### 6.5. Dataportabilitet og »retten til at blive gemt«

83. Dataportabilitet og »retten til at blive glemt« er to med hinanden forbundne koncepter, der fremsættes i medde-

lelsen med henblik på at styrke de registreredes rettigheder. De supplerer de principper, der allerede er nævnt i direktivet, som giver den registrerede ret til at gøre indsigelse mod den yderligere behandling af hans/hendes personoplysninger og en forpligtelse for den registeransvarlige til at slette oplysninger, så snart de ikke længere er nødvendige for behandlingens formål.

84. Disse to begreber har mest merværdi i en informations-samfundsmæssig kontekst, hvor flere og flere data gemmes automatisk og opbevares i et ubestemt tidsrum. Praksis viser, at selv om data uploades af den registrerede selv, er den grad af kontrol, som den pågældende effektivt har over sine personoplysninger, i realiteten meget begrænset. Det er endnu mere sandt i lyset af den gigantiske hukommelse, som internettet repræsenterer i dag. Desuden er det ud fra et økonomisk perspektiv mere omkostningskrævende for en registeransvarlig at slette data end fortsat at opbevare dem. Udøvelsen af den enkeltes rettigheder går derfor imod den naturlige økonomiske trend.
85. Både dataportabilitet og »retten til at blive glemt« kunne bidrage til at tippe balancen til fordel for den registrerede. Målet for dataportabiliteten ville være at give mere kontrol til den enkelte over egne oplysninger, mens »retten til at blive glemt« ville sikre, at oplysningerne automatisk forsvinder efter en vis periode, også selv om den registrerede ikke foretager sig noget i den anledning, eller hvis denne slet ikke er klar over, at oplysningerne nogensinde har været lagret.
86. Mere specifikt forstås der ved dataportabilitet brugernes mulighed for at ændre præference for behandlingen af deres data, især i forbindelse med nye teknologiudelser. Dette gælder i stigende grad for ydelser, som indebærer lagring af oplysninger, herunder personoplysninger såsom mobiltelefoni og ydelser, hvori indgår lagring af billeder, e-mails og andre oplysninger, undertiden ved hjælp af cloud computing-ydelser.
87. Enkelt personer skal nemt og frit kunne skifte udbyder og overføre deres personoplysninger til en anden serviceudbyder. EDPS mener, at de eksisterende rettigheder, der er fastsat i direktiv 95/46/EF, kunne styrkes ved at indsætte portabilitetsrettigheder, især i forbindelse med informations-samfundstjenester, for at bistå enkelt personer med at sikre, at udbydere og andre relevante registeransvarlige giver dem adgang til deres personoplysninger, mens det samtidig sikres, at gamle udbydere eller andre registeransvarlige sletter disse oplysninger, selv om de gerne ville beholde dem til deres egne legitime formål.

88. En nyligt kodificeret »ret til at blive glemt« ville sikre sletningen af personoplysninger eller et forbud mod fortsat anvendelse heraf uden en nødvendig handling fra den registreredes side, men på den betingelse, at disse data allerede har været opbevaret i et vist tidsrum. Dataene ville med andre ord blive tildelt en slags udløbsdato. Dette

<sup>(39)</sup> Artikel 29-Gruppen arbejder i øjeblikket på en udtalelse om »samtykke«. Denne udtalelse kan afstedkomme yderligere forslag.

princip er allerede bekræftet i nationale domstolssager eller anvendt inden for specifikke sektorer, f.eks. i forbindelse med politisager, straffeattester eller disciplinærsager: I henhold til nogle nationale lovgivninger slettes oplysninger om enkeltpersoner automatisk eller må ikke videregives eller -formidles, navnlig efter en bestemt periode, uden behov for en forudgående analyse på et sag til sag-grundlag.

89. I den forstand skal en ny »ret til at blive glemt« knyttes til dataportabilitet. Den merværdi, som det ville medføre, er, at det ikke ville kræve bestræbelser eller insistere fra den registrerede at få sine data slettet, da dette ville ske på en objektiv og automatiseret måde. Kun under meget særlige omstændigheder, hvor der kan konstateres et specifikt behov for at opbevare data længere, kan en registeransvarlig være berettiget til at opbevare dataene. »Retten til at blive glemt« ville således vende bevisbyrden fra den enkelte til den registeransvarlige og udgøre en »privacy by default«-indstilling (privatlivsvenlig standardindstilling) ved behandlingen af personoplysninger.

90. EDPS er af den opfattelse, at »retten til at blive glemt« vil kunne vise sig at være specielt nyttig i forbindelse med informationssamfundstjenester. En forpligtelse til at slette eller ikke videreformidle oplysninger efter en bestemt periode giver mening, særligt i medierne eller på internettet og især i sociale netværk. Det ville også være nyttigt for så vidt angår terminaludstyr: data opbevaret på mobile anordninger eller computere ville automatisk blive slettet eller blokeret efter en bestemt periode, når de ikke længere er i den enkeltes besiddelse. På den baggrund kan »retten til at blive glemt« oversættes til en »privacy by design«-forpligtelse.

91. Kort sagt mener EDPS, at dataportabilitet og »retten til at blive glemt« er nyttige koncepter. Det vil kunne betale sig at inddrage dem i det retlige instrument, men sandsynligvis begrænset til det elektroniske samfund.

#### 6.6. Behandling af personoplysninger vedrørende børn

92. I henhold til direktiv 95/46/EF er der ikke nogen særlige regler vedrørende behandlingen af børns personoplysninger. Heri anerkendes behovet ikke for en særlig beskyttelse af børn under specifikke omstændigheder, på grund af deres sårbarhed, og fordi det skaber retsikkerhed, især på følgende områder:

- Indsamlingen af børns personoplysninger og den måde, hvorpå de skal informeres om indsamlingen
- Den måde, hvorpå børns samtykke indhentes. Fordi der ikke er nogen særlige regler om, hvordan børns samtykke opnås, og aldersgrænse for, hvornår børn kan anses som sådan, behandles disse spørgsmål i henhold til den nationale lovgivning, som er forskellig

fra medlemsstat til medlemsstat<sup>(40)</sup>

- Den måde og de betingelser, i henhold til hvilke børn eller deres retlige repræsentanter kan udøve deres rettigheder i henhold til direktivet.

93. EDPS vurderer, at børns særlige interesser ville være bedre beskyttet, hvis det nye retlige instrument indeholdt yderligere bestemmelser, der specifikt omhandler indsamlingen og den videre behandling af børns personoplysninger. Sådanne særlige bestemmelser ville desuden give retssikkerhed på dette specifikke område, og de ville være en fordel for registeransvarlige, hvortil der på nuværende tidspunkt stilles forskellige lovgivningsmæssige krav.

94. EDPS foreslår at indsætte følgende bestemmelser i det retlige instrument:

- Et krav om, at oplysninger skal tilpasses til børn, for så vidt dette ville gøre det nemmere for børn at forstå, hvad det betyder, når der indsamles oplysninger om dem.
- Andre oplysningskrav tilpasset til børn til, hvordan oplysningerne skal gives og eventuelt også til indholdet.
- En særlig bestemmelse, der beskytter børn mod adfærdsbetinget reklamering.
- Formålsbegrænsningsprincippet skal styrkes, for så vidt angår børns data.
- Nogle kategorier af data skal aldrig indsamles fra børn.
- En aldersgrænse. Under en sådan grænse skal der almindeligvis kun indsamles oplysninger fra børn, hvis der foreligger eksplicit og verificerbart forældresamtykke.
- Hvis forældresamtykke er nødvendig, ville det være påkrævet at fastsætte regler for, hvordan barnets alder bekræftes, dvs., hvordan det fastslås, at barnet

<sup>(40)</sup> Samtykke er normalt forbundet med den alder, hvor børn kan indgå kontraktlige forpligtelser. Hermed menes den alder, hvor børn formodes at have nået et vist modenhedsniveau. Eksempelvis kræver spansk lovgivning samtykke fra forældre til at indsamle personoplysninger om børn, som endnu ikke er fyldt 14 år. Over denne alder anses børn for at kunne afgive samtykke. I Det Forenede Kongerige henviser databeskyttelsesloven ikke til en bestemt alder eller grænse. Det Forenede Kongeriges databeskyttelsesmyndighed har imidlertid fortolket det således, at børn over 12 kan afgive samtykke. Omvendt kan børn under 12 ikke afgive samtykke, og med henblik på at få adgang til deres personlige oplysninger er det nødvendigt at indhente tilladelse fra en forælder eller værge.

er mindreårigt, og hvordan forældresamtykke verificeres. Det er et område, hvor EU kan få inspiration fra andre lande, f.eks. USA <sup>(41)</sup>.

#### 6.7. Mekanismer for kollektiv søgsmålsadgang

95. En styrkelse af indholdet i enkeltpersoners rettigheder ville ikke give mening, idet der ikke findes effektive procedurer til at håndhæve sådanne rettigheder. I den forbindelse anbefaler EDPS indførelsen i EU-lovgivningen af mekanismer for kollektiv søgsmålsadgang i forbindelse med brud på databeskyttelsesregler. Navnlig kan mekanismer for kollektiv søgsmålsadgang, der giver grupper af borgere bemyndigelse til at kombinere deres krav i ét enkelt søgsmål, være et meget magtfuldt redskab til at fremme håndhævelsen af databeskyttelsesreglerne <sup>(42)</sup>. Denne innovation støttes også af databeskyttelsesmyndighederne i arbejdsgruppens dokument om fremtiden for privatlivets fred.

96. I sager med mindre følger er det usandsynligt, at ofrene for et brud på databeskyttelsesreglerne ville anlægge individuelle søgsmål mod de registeransvarlige set i lyset af de omkostninger, forsinkelser, usikkerheder, risici og byrder, de ville blive udsat for. Disse vanskeligheder ville kunne løses eller afbødes væsentligt, hvis der var et system for kollektiv søgsmålsadgang til rådighed, som bemyndiger ofrene for sikkerhedsbrud til at samle deres individuelle krav i ét enkelt søgsmål. EDPS ville også tilgodese godkendte organers ansvar, f.eks. forbrugerorganisationer eller offentlige organer, til at anlægge erstatningsøgsmål på vegne af ofre for brud på datasikkerhedsreglerne. Disse søgsmål bør ikke berøre den registreredes ret til at anlægge individuelle søgsmål.

97. Ikke alene er kollektive søgsmål vigtige for at sikre fuld compensation eller andre afhjælpende foranstaltninger, men de har også indirekte en øget afskrækkelsesfunktion. Risikoen for at skulle afholde dyre kollektive erstatninger i sådanne søgsmål ville mangedoble de registeransvarliges incitamentet til at sikre overensstemmelse. Med hensyn hertil ville en øget privat håndhævelse ved hjælp af mekanismer for kollektiv søgsmålsadgang supplere den offentlige håndhævelse.

98. Meddelelsen tager ikke stilling i dette spørgsmål. EDPS er opmærksom på de igangværende forhandlinger på europæisk plan om indførelsen af kollektiv søgsmålsadgang

for forbrugere. Han er også bevidst om risikoen for tilbagebetalinger, som disse mekanismer kan medføre på basis af erfaringerne i andre retssystemer. Efter hans vurdering er disse faktorer imidlertid ikke et tilstrækkeligt argument for at afvise eller udsætte indførelsen heraf i databeskyttelseslovgivningen, hvilket skal ses i lyset af de fordele, som de ville indebære <sup>(43)</sup>.

## 7. Styrkelse af organisationernes/de registeransvarliges rolle

### 7.1. Generelt

99. EDPS er af den opfattelse, at ud over at styrke enkeltpersoners rettigheder skal et moderne retligt instrument til regulering af databeskyttelsen indeholde de nødvendige redskaber, som øger de registeransvarliges ansvar. Nærmere bestemt skal rammen indeholde incitamentet for registeransvarlige i den private eller offentlige sektor til proaktivt at inddrage databeskyttelsesforanstaltninger i deres arbejdsgange. Disse redskaber ville for det første være nyttige, fordi, som det blev nævnt tidligere, den teknologiske udvikling resulterede i en stærk vækst i indsamlingen, anvendelsen og yderligere overførsel af personoplysninger, hvilket forøger risiciene for privatlivets fred og beskyttelsen af enkeltpersoners personoplysninger, hvilket skal kompenseres på en effektiv måde. For det andet mangler den nuværende ramme — undtagen i nogle få veldefinerede bestemmelser (se nedenfor) — sådanne redskaber, og de registeransvarlige kan anlægge en reaktiv tilgang til databeskyttelse og privatlivets fred, og således kun reagere efter, at et problem er opstået. Denne tilgang afspejles i statistikker, der viser dårlige overensstemmelsespraksisser og datatab som et tilbagevendende problem.

100. Ifølge EDPS er den eksisterende ramme ikke tilstrækkelig til at beskytte personoplysninger effektivt under de nuværende og fremtidige forhold. Jo højere risici, desto større er behovet for at gennemføre konkrete foranstaltninger, der beskytter oplysninger på et praktisk niveau og giver effektiv beskyttelse. Medmindre disse proaktive foranstaltninger reelt gennemføres, vil fejl, uheld og forsømmelser sandsynligvis fortsætte, hvilket bringer enkeltpersoners ret til privatlivets fred i fare i det stadigt mere digitale samfund. Med henblik på at opnå dette foreslår EDPS følgende foranstaltninger.

### 7.2. Styrkelse af de registeransvarliges ansvarlighed

101. EDPS anbefaler, at der tilføjes en ny bestemmelse i det retlige instrument med krav om, at registeransvarlige skal gennemføre relevante og effektive foranstaltninger til indførelse af principperne og forpligtelserne i det retlige instrument og påvise dette på forlangende.

<sup>(41)</sup> I USA kræver COOPA, at operatører af kommercielle websteder eller onlinetjenester rettet mod børn under 13 skal indhente samtykke fra forældre, før der sker indsamling af personlige oplysninger, og at operatører af kommercielle alment tilgængelige websteder skal have konkret kendskab til, at nogle af de besøgende er børn.

<sup>(42)</sup> Se også Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse af 25. juli 2007 om Kommissionens meddelelse til Europa-Parlamentet og Rådet vedrørende opfølgningen på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet, EUT C 255 af 27.10.2007, s. 10.

<sup>(43)</sup> Nogle nationale lovgivninger indeholder allerede lignende mekanismer.

102. Denne type bestemmelse er ikke fuldkommen ny. Artikel 6, stk. 2, i direktiv 95/46/EF henviser til principperne vedrørende datakvalitet og nævner, at »Det påhviler den registeransvarlige at sikre, at stk. 1 overholdes«. Tilsvarende kræver artikel 17, stk. 1, at de registeransvarlige gennemfører foranstaltninger af både teknisk og organisatorisk art. Disse bestemmelser har imidlertid begrænset omfang. Indsættelse af en generel bestemmelse om ansvarlighed ville animere registeransvarlige til at træffe proaktive foranstaltninger med henblik på at kunne overholde alle elementerne i databeskyttelseslovgivningen.
103. En bestemmelse om ansvarlighed ville have den konsekvens, at registeransvarlige skal indføre interne mekanismer og kontrolsystemer, som sikrer overholdelse af principperne og forpligtelserne i rammen. Dette ville f.eks. kræve, at den øverste ledelse involveres i databeskyttelsespolitikker, kortlægningsprocedurer for at sikre korrekt identifikation af alle databehandlingsoperationer, have bindende databeskyttelsespolitikker, som også kontinuerligt skal gennemgås og opdateres med henblik på at omfatte nye databehandlingsoperationer og overholde principperne vedrørende datakvalitet, underretning, sikkerhed, adgang osv. Det ville også kræve, at de registeransvarlige opbevarer dokumentation for at kunne påvise overensstemmelse til myndighederne på forlangende. At påvise overensstemmelse i forhold til den brede offentlighed bør i visse tilfælde også gøres obligatorisk. Dette vil kunne gøres ved eksempelvis at kræve, at de registeransvarlige skal inkorporere databeskyttelse i offentlige (årlige) rapporter, hvis sådanne rapporter er obligatoriske af andre grunde.
104. Det er klart, at de typer af interne og eksterne foranstaltninger, der skal gennemføres, skal være passende og afhænge af de faktiske forhold og omstændigheder i hver enkelt sag. Det gør en forskel, om en registeransvarlig behandler nogle få hundrede kundefortegnelser, som hovedsagelig består af navne og adresser, eller om den pågældende behandler journaler for millioner af patienter, herunder deres sygehistorie. Det samme gælder for de specifikke måder, hvorpå effektiviteten af foranstaltningerne skal vurderes. Der er behov for skalérbarhed.
105. Det samlede generelle retlige instrument for databeskyttelse skal ikke fastsætte de specifikke krav til ansvarlighed, men kun dens væsentlige elementer. Meddelelsen fastsætter bestemte elementer til styrkelse af de registeransvarliges ansvar, som er meget velkomne. Nærmere bestemt støtter EDPS fuldt ud, at anvendelsen af databeskyttelsesansvarlige og »privatlivskonsekvensanalyser« (Privacy Impact Assessments (PIA)) gøres obligatorisk, inden for visse fastlagte grænser.
106. Derudover anbefaler EDPS at uddelegere beføjelser til Kommissionen i henhold til EUF-traktatens artikel 290 for at supplere de grundlæggende krav, der er nødvendige for at overholde ansvarlighedsstandarderne. Anvendelse af disse beføjelser ville øge de registeransvarliges retssikkerhed og harmonisere overensstemmelse i hele EU. I forbindelse med udviklingen af sådanne specifikke instrumenter skal Artikel 29-Gruppen og EDPS høres.
107. Endelig ville de konkrete ansvarlighedsforanstaltninger, der skal gennemføres af registeransvarlige, også kunne pålægges af databeskyttelsesmyndighederne som led i deres håndhævelsesbeføjelser. Med henblik herpå skal databeskyttelsesmyndighederne gives nye beføjelser, som sætter dem i stand til at pålægge afhjælpningsforanstaltninger eller sanktioner. Eksempler bør omfatte etableringen af interne overensstemmelsesprogrammer, at implementere »privacy by design« i specifikke produkter og tjenesteydelser osv. Der bør kun pålægges foranstaltninger, for så vidt de er relevante, forholdsmæssige og effektive med henblik på at sikre overensstemmelse med gældende og håndhævede retsnormer.

### 7.3. »Privacy by design«

108. »Privacy by design« henviser til integrationen af databeskyttelse og privatlivets fred helt fra starten af nye produkter, ydelser og procedurer, der indebærer behandling af personoplysninger. Ifølge EDPS er »privacy by design« et element af ansvarlighed. I overensstemmelse hermed ville de registeransvarlige også skulle godtgøre, at de havde implementeret »privacy by design«, hvor det er relevant. For nylig vedtog den 32. internationale konference mellem datatilsynsmyndighederne en resolution, der anerkender »privacy by design«-princippet som et væsentligt element i den grundlæggende beskyttelse af privatlivets fred<sup>(44)</sup>.
109. Direktiv 95/46/EF indeholder nogle bestemmelser til fremme af »privacy by design«<sup>(45)</sup>, men anerkender ikke direkte en sådan forpligtelse. EDPS er tilfreds med meddelelsens godkendelse af »privacy by design«-princippet som et redskab til at sikre overholdelse af databeskyttelsesreglerne. Han foreslår, at der indsættes en bindende bestemmelse, som fastsætter en »privacy by design«-forpligtelse, der ville kunne baseres på ordlyden i betragtning 46 i

<sup>(44)</sup> Resolution om »Privacy by Design«, vedtaget af den 32. internationale konference mellem datatilsynsmyndighederne, Jerusalem d. 27.-29. oktober 2010.

<sup>(45)</sup> Direktivet omfatter bestemmelser, der indirekte, i forskellige situationer, kræver gennemførelsen af »privacy by design«. Navnlig artikel 17 kræver, at registeransvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at forhindre ulovlig databehandling. E-direktivet om privatlivets fred er mere eksplicit. I artikel 14.3 hedder det: »Hvor der er behov herfor, kan der vedtages foranstaltninger for at sikre, at terminaludstyr fremstilles på en måde, der er forenelig med brugernes ret til at beskytte og kontrollere anvendelsen af deres personoplysninger i overensstemmelse med direktiv 1999/5/EF og Rådets beslutning 87/95/EØF af 22. december 1986 om standardisering inden for informationsteknologi og telekommunikation«.

direktiv 95/46/EF. Mere specifikt ville bestemmelsen udtrykkeligt kræve, at de registeransvarlige gennemfører tekniske og organisatoriske foranstaltninger, både på tidspunktet for udformningen af behandlingssystemet og på tidspunktet for selve behandlingen, navnlig med henblik på at sikre beskyttelsen af personoplysninger og forhindre uautoriseret behandling <sup>(46)</sup>.

110. På grundlag af en sådan bestemmelse ville de registeransvarlige bl.a. skulle sikre, at databehandlingsystemerne udformes til at behandle så få personoplysninger som muligt, implementere »privacy by default«-indstillinger, f.eks. i sociale netværk, at opbevare enkeltpersoners profiler således, at de som standard er utilgængelige for andre, samt at implementere redskaber, der gør det muligt for brugerne at opnå en bedre beskyttelse af deres personoplysninger (f.eks. adgangskontroller, kryptering).

111. Fordelene ved en mere eksplicit henvisning til »privacy by design« kan opsummeres som følger:

— Det ville fremhæve vigtigheden af princippet *per se* som et redskab til at sikre, at processer, produkter og tjenesteydelser fra starten er udformet med databeskyttelse for øje.

— Det ville reducere misbrug af privatlivets fred, og det ville minimere den unødvendige indsamling af data og bemyndige enkeltpersoner til at træffe reelle valg vedrørende deres personoplysninger.

— Det ville forhindre, at der på et senere tidspunkt skulle iværksættes »støtteforanstaltninger« i et forsøg på at løse problemer, der kan være vanskelige, hvis ikke umulige, at afhjælpe.

— Det ville også fremme databeskyttelsesmyndighedernes effektive anvendelse og håndhævelse af dette princip.

112. Den kombinerede virkning af denne forpligtelse ville resultere i en større efterspørgsel efter »privacy by design«-produkter og -tjenesteydelser, hvilket skulle skabe flere incitamenter for industrien til at opfylde en sådan efterspørgsel. Det bør endvidere overvejes at fastsætte en særskilt forpligtelse rettet mod designere og producenter af nye produkter og tjenesteydelser med sandsynlig indvirkning på databeskyttelse og privatlivets fred. EDPS foreslår at inddrage en sådan særskilt forpligtelse, der vil bidrage yderligere til, at de registeransvarlige kan opfylde deres egen forpligtelse.

113. Kodificeringen af »privacy by design« (indbygget databeskyttelse) kan suppleres med en bestemmelse, som fastsætter generelle krav til den indbyggede databeskyttelse,

der gælder på tværs af sektorer, produkter og tjenesteydelser, f.eks. at sikre brugeren bemyndigelsesforanstaltninger, som skal vedtages i henhold til princippet.

114. Desuden anbefaler EDPS at uddelegere beføjelser til Kommissionen i henhold til EUF-traktatens artikel 290 for — hvor det er relevant — at supplere de grundlæggende krav vedrørende den indbyggede databeskyttelse for udvalgte produkter og tjenesteydelser. Anvendelse af disse beføjelser ville forbedre de registeransvarliges retssikkerhed og harmonisere overensstemmelse i hele EU. I forbindelse med udviklingen af sådanne specifikke instrumenter skal Artikel 29-Gruppen og EDPS høres (se også punkt 106 om ansvarlighed).

115. Endelig skal databeskyttelsesmyndighederne gives beføjelse til at pålægge afhjælpningsforanstaltninger eller sanktioner i henhold til lignende restriktive betingelser som omhandlet i punkt 107, hvor de registeransvarlige tydeligt har undladt at træffe konkrete foranstaltninger i sager, hvor dette ville være påkrævet.

#### 7.4. Certificeringstjenesteydelser

116. Meddelelsen anerkender behovet for at undersøge udarbejdelsen af EU-certificeringsordninger for produkter og tjenesteydelser, der sikrer privatlivets fred. EDPS støtter fuldt ud dette mål og foreslår at indsætte en bestemmelse med henblik på at tilvejebringe disse og mulige virkninger på tværs af EU, som kan udvikles yderligere i en tillægsbestemmelse på et senere tidspunkt. Bestemmelsen skal supplere bestemmelserne om ansvarlighed og »privacy by design«.

117. Frivillige certificeringssystemer ville muliggøre verificering af, at en registeransvarlig har truffet foranstaltninger til at overholde det retlige instrument. Derudover vil registeransvarlige — eller endog produkter eller tjenesteydelser — der nyder godt af et certificeringsmærke kunne få en konkurrencemæssig fordel i forhold til andre. Sådanne ordninger ville også bistå databeskyttelsesmyndighederne i deres tilsyns- og håndhævelsesrolle.

## 8. Globalisering og gældende lov

### 8.1. Et klart behov for mere ensartet beskyttelse

118. Som nævnt tidligere i afsnit 2, er overførslen af personoplysninger uden for EU's grænser steget eksponentielt som et resultat af udviklingen af nye teknologier, de multinationale virksomheders rolle og regeringernes voksende indflydelse i forbindelse med behandlingen og delingen af personoplysninger på internationalt plan. Dette er et af de vigtigste forhold, der berettiger revisionen af den nuværende retlige ramme. Derfor er det et af de områder, hvor EDPS efterspørger ambitioner og effektivitet, da der er et klart behov for en mere ensartet beskyttelse, når data behandles uden for EU.

<sup>(46)</sup> I henhold til den nuværende ramme opfordrer betragtning 46 de registeransvarlige til at gennemføre sådanne foranstaltninger, men en betragtning har naturligvis ikke bindende virkning.

### 8.2. Investering i internationale regler

119. Ifølge EDPS er der behov for flere investeringer i forbindelse med udviklingen af internationale regler. Mere harmonisering med hensyn til niveauet for beskyttelse af personoplysninger på verdensplan ville i betydelig grad tydeliggøre indholdet af de principper, der skal overholdes, og betingelserne for overførsel af data. Disse globale regler ville skulle forene kravet om en højere standard for databeskyttelse — herunder kerneelementer i EU's databeskyttelse — med regionale specificiteter.
120. EDPS støtter det ambitiøse arbejde, der indtil nu er udført inden for rammerne af den internationale konference mellem datatilsynsmyndighederne, med at udvikle og formidle de såkaldte Madridstandarder med henblik på at inkorporere dem i et bindende instrument og eventuelt afholde en regeringskonference<sup>(47)</sup>. Han opfordrer Kommissionen til at tage de nødvendige initiativer til at fremme gennemførelsen af dette mål.
121. EDPS mener, at det ligeledes er vigtigt at sikre sammenhæng mellem dette initiativ til internationale standarder, den aktuelle revurdering af EU's ramme for databeskyttelse og andre udviklinger, f.eks. den nuværende revision af OECD's retningslinjer for beskyttelse af privatlivets fred og af Europarådets konvention 108, som er åben for undertegnelse af tredjelande (se også punkt 17). EDPS finder, at Kommissionen har en særlig rolle at spille her ved at angive, hvordan den vil fremme en sådan sammenhæng under forhandlingerne i OECD og Europarådet.

### 8.3. Præcisering af kriterier for gældende lov

122. Da det er svært at opnå fuldstændig sammenhæng, for der vil — i det mindste i den nærmeste fremtid — fortsat være en vis forskel mellem lovgivningerne inden for EU og med desto større ret uden for EU's grænser. EDPS finder, at et nyt retligt instrument skal præcisere kriterierne for afgørelsen af, hvilken lovgivning der finder anvendelse, og sikre strømlinede mekanismer for datastrømme samt ansvarligheden for de aktører, der er involveret i datastrømme.
123. For det første skal det retlige instrument sikre, at EU-lovgivning er gældende, når personoplysninger behandles uden for EU's grænser, men hvor der er et berettiget krav om anvendelse af EU-lovgivning. Eksemplet med ikkeeuropæiske cloud computing-ydelser, der er rettet mod EU-borgere illustrerer, hvorfor dette er nødvendigt. I et samfund, hvor data ikke opbevares fysisk og behandles på et fast sted, hvor serviceudbydere og brugere i forskellige lande har interfererende indflydelse på data, er det meget vanskeligt at identificere, hvem der er ansvarlig for at overholde hvilke databeskyttelsesprincipper. Der

gives vejledning om, især af databeskyttelsesmyndighederne, hvordan direktiv 95/46/EF skal fortolkes og anvendes i sådanne tilfælde, men vejledning alene er ikke nok til at sikre retssikkerhed i dette nye samfund.

124. Inden for EU's område er behovet for mere præcision i den retlige ramme og et forenklet kriterium til at afgøre, hvilken lov der finder anvendelse, blevet fremhævet af Artikel 29-Gruppen i en nylig udtalelse<sup>(48)</sup>.
125. Ifølge EDPS ville den foretrukne mulighed være at fastsætte det retlige instrument i en forordning, hvilket ville betyde, at der gælder identiske regler i alle medlemsstater. En forordning ville gøre behovet for fastlæggelse af gældende lovgivning mindre vigtigt. Det er en af grundene til, at EDPS advokerer kraftigt for vedtagelsen af en forordning. Men en forordning vil imidlertid også kunne give en vis manøvremargin for medlemsstaterne. Hvis der bevares en vis manøvremargin i det nye instrument, vil EDPS støtte forslaget fra Artikel 29-Gruppen om at skifte fra en distributiv anvendelse af forskellige nationale lovgivninger til en centraliseret anvendelse af én enkelt lovgivning i alle medlemsstater, hvor en registeransvarlig har virksomheder. Han plæderer også for mere samarbejde og samordning mellem dataskyttelsesmyndighederne i tværnationale sager og klager (se afsnit 10).

### 8.4. Strømning af mekanismer for datastrømme

126. Behovet for sammenhæng og for en højniveau-benchmark skal ikke kun tages i betragtning med henblik på globale databeskyttelsesprincipper, men også for så vidt angår internationale overførsler. EDPS støtter fuldt ud Kommissionens mål om at strømline nuværende procedurer for internationale dataoverførsler og sikre en mere fælles og sammenhængende tilgang i forhold til tredjelande og internationale organisationer.
127. Mekanismerne for datastrømme omfatter både den private sektors overførsler, især via kontraktklausuler eller bindende virksomhedsregler samt overførsler mellem offentlige myndigheder. Bindende virksomhedsregler er et af de elementer, hvor en mere sammenhængende og strømlinet tilgang ville være ønskelig. EDPS anbefaler at tage fat på betingelserne for virksomhedsregler på en eksplicit måde i det nye retlige instrument<sup>(49)</sup> ved at:
- eksplicit anerkende bindende virksomhedsregler som redskaber, der giver de fornødne retlige garantier
  - fastsætte de vigtigste elementer/betingelser i forbindelse med vedtagelsen af bindende virksomhedsregler

<sup>(47)</sup> Som foreslået ved resolution om internationale standarder, vedtaget af den 32. internationale konference mellem datatilsynsmyndighederne, Jerusalem d. 27.-29. oktober 2010.

<sup>(48)</sup> Udtalelse fra Artikel 29-Gruppen 8/2010 om gældende lov, arbejdsgruppens dokument 179.

<sup>(49)</sup> Vedrørende internationale overførsler, se også afsnit 8 i denne udtalelse.



- fastlægge samarbejdsprocedurer for vedtagelsen af bindende virksomhedsregler, herunder kriterier for valg af én ledende tilsynsmyndighed («one-stop-shop»-princippet).

## 9. Politi og retsvæsen

### 9.1. Det generelle instrument

128. Kommissionen har gentagne gange understreget vigtigheden af at styrke databeskyttelsen i forbindelse med retshåndhævelse og kriminalitetsforebyggelse, fordi udvekslingen af personoplysninger er blevet væsentligt intensiveret. Også Stockholmprogrammet, der er godkendt af Det Europæiske Råd, henviser til et solidt databeskyttelses-system som den væsentligste forudsætning for EU's informationsstyringsstrategi på dette område<sup>(50)</sup>.
129. Revurderingen af den generelle databeskyttelsesramme er den perfekte anledning til at gøre fremskridt i den henseende, navnlig da meddelelsen med rette beskriver rammeafgørelse 2008/977 som utilstrækkelig<sup>(51)</sup>.
130. EDPS anførte i afsnit 3.2.5 i denne udtalelse, hvorfor samarbejdet mellem politi og retsvæsen skulle inddrages i det generelle instrument. Inddragelsen af politi og retsvæsen har en række yderligere fordele. Det betyder, at reglerne ikke længere kun vil gælde for grænseoverskridende dataoverførsler<sup>(52)</sup>, men også for indenlandsk databehandling. Tilstrækkelig beskyttelse i forbindelse med udveksling af personoplysninger med tredjelande vil bedre kunne sikres, også for så vidt angår internationale aftaler. Derudover vil databeskyttelsesmyndighederne have de samme omfattende og harmoniserede beføjelser i forhold til politi- og retsmyndigheder som de har i forhold til andre registeransvarlige. Endelig skal den nuværende artikel 13, der giver medlemsstaterne beføjelse til at vedtage specifik lovgivning for at begrænse forpligtelser og rettigheder i henhold til det generelle instrument for særlig offentlig interesse, anvendes på den samme restriktive måde, som den anvendes på andre områder. Især skal de særlige sikkerhedsregler, der er fastsat i henhold til det generelle instrument på dette område, også overholdes i den nationale lovgivning, der vedtages inden for det politimæssige og strafferetlige samarbejde.

### 9.2. Yderligere særegler for politi og retsvæsen

131. En sådan inddragelse vil imidlertid ikke udelukke særegler og afvigelser, som tager behørigt hensyn til denne sektors specificiteter i overensstemmelse med erklæring 21, der er knyttet til Lissabontraktaten. Begrænsninger i registreredes

rettigheder kan fastsættes, men de skal være nødvendige, forholdsmæssige og ikke ændre de væsentlige elementer i selve rettigheden. Det skal i denne sammenhæng understreges, at direktiv 95/46/EF, herunder dets artikel 13, på nuværende tidspunkt gælder for retshåndhævelsen på forskellige områder (f.eks. skat, told, svig), der ikke er grundlæggende forskellige fra mange aktiviteter inden for det politimæssige og strafferetlige samarbejde.

132. Desuden skal der også indføres særlige sikkerhedsregler med henblik på at kompensere den registrerede ved at give ham yderligere beskyttelse på et område, hvor der er større risiko for, at behandlingen af personoplysninger kan være krænkende.

133. I lyset af det ovenstående vurderer EDPS, at den nye ramme i overensstemmelse med konvention 108 og anbefaling nr. R (87) 15 skal omfatte som minimum følgende elementer:

- En sontring mellem forskellige kategorier af data og filer i henhold til deres nøjagtighed og pålidelighed, og støtte til princippet om, at der skal foretages en skelnen mellem data baseret på fakta og data baseret på personlige opfattelser eller vurderinger.
- En sontring mellem forskellige kategorier af registrerede (personer, der er mistænkt for at have begået kriminelle handlinger, ofre, vidner osv.) og dokumenter (midlertidige, blivende og efterretningsdokumenter). Der må påregnes særlige forhold og sikkerhedsforanstaltninger i forbindelse med behandling af ikkeregistrerede.
- Mekanismer til at sikre periodisk verificering og fejludbedring for at sikre kvaliteten af de data, der behandles.
- Særlige bestemmelser og/eller sikkerhedsforanstaltninger kan udarbejdes i relation til den (stadigt mere relevante) behandling af biometriske og genetiske data inden for retshåndhævelsesområdet. Anvendelsen heraf skal begrænses til tilfælde, hvor der ikke er nogen mindre aggressive virkemidler til rådighed, som kan have den samme virkning<sup>(53)</sup>.
- Betingelser for overførsel af personoplysninger til ikke-kompetente myndigheder og private parter samt for adgang og retshåndhævelsesmyndighedernes yderligere anvendelse af personoplysninger, der er indsamlet af private parter.

<sup>(50)</sup> Se herom udtalelse fra EDPS af 30. september 2010 om Kommissionens meddelelse til Europa-Parlamentet og Rådet — »Oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed«, punkt 9-19.

<sup>(51)</sup> Se afsnit 3.2.5 ovenfor.

<sup>(52)</sup> Dette er i øjeblikket det begrænsede omfang af rammeafgørelse 2008/977.

<sup>(53)</sup> Se i den forbindelse arbejdsgruppens dokument om fremtiden for privatlivets fred, punkt 112.

### 9.3. Sektorspecifikke databeskyttelsesordninger

134. I meddelelsen hedder det, at »rammeafgørelsen ikke afløser de forskellige sektorspecifikke lovgivningsmæssige instrumenter inden for det politimæssige og strafferetlige samarbejde, som er vedtaget på EU-niveau, særlig de instrumenter, der fastlægger Europol's, Eurojust's, Schengeninformationssystemets og toldinformationssystemets funktionsmåde, og som enten har særlige databeskyttelsesordninger, og/eller som normalt henviser til Europarådets databeskyttelsesinstrumenter.
135. EDPS mener, at den nye retlige ramme så vidt muligt skal være klar, enkel og sammenhængende. Hvis der sker en spredning af forskellige ordninger, der gælder for f.eks. Europol, Eurojust, SIS and Prüm, vil det fortsat være kompliceret eller endog blive endnu mere kompliceret at opnå overensstemmelse med reglerne. Det er en af grundene til, at EDPS foretrækker ét samlet retligt instrument for alle sektorer.
136. EDPS er imidlertid klar over, at en ensretning af reglerne fra de forskellige systemer kræver meget arbejde, som skal udføres omhyggeligt. EDPS er af den opfattelse, at en gradvis tilgang som nævnt i meddelelsen giver mening, så længe forpligtelsen til at sikre et højt databeskyttelsesniveau på en ensartet og effektiv måde forbliver klar og synlig. For at være mere konkret:
- I et første stade skal det generelle retlige instrument for databeskyttelse gøres anvendelig for al databehandling inden for det politimæssige og strafferetlige samarbejde, herunder justeringerne for politi og retsvæsen (jf. 9.2).
  - I et andet stade skal de sektorspecifikke databeskyttelsesordninger rettes ind efter det generelle instrument. Kommissionen skal forpligte sig til at vedtage forslag til dette andet stade inden for en kort og angivet tidsramme.

## 10. Databeskyttelsesmyndigheder og samarbejdet mellem databeskyttelsesmyndigheder

### 10.1. Styrkelse af databeskyttelsesmyndighedernes rolle

137. EDPS støtter fuldt ud Kommissionens mål om at behandle spørgsmålet om databeskyttelsesmyndighedernes status og mere eksplicit om at styrke deres uafhængighed, ressourcer og håndhævelsesbeføjelser.
138. EDPS insisterer desuden på behovet for at præcisere det væsentlige begreb vedrørende databeskyttelsesmyndighedernes uafhængighed i det nye retlige instrument. EF-Domstolen har for nylig truffet en afgørelse om dette emne i sag C-518/07<sup>(54)</sup>, hvor den betonede, at uafhængighed betyder fraværet af enhver form for udefra

kommende påvirkning. En databeskyttelsesmyndighed må hverken søge eller modtage instruktioner fra nogen. EDPS foreslår eksplicit at kodificere disse elementer af uafhængighed i lovgivningen.

139. For at kunne udøve deres opgaver skal databeskyttelsesmyndighederne tildeles tilstrækkelige menneskelige og økonomiske ressourcer. EDPS foreslår at indsætte dette krav i lovgivningen<sup>(55)</sup>. Afslutningsvis fremhæver han behovet for at sikre, at myndighederne har fuldt harmoniserede beføjelser med hensyn til undersøgelse og pålæggelse af tilstrækkeligt afskrækkende og afhjælpende foranstaltninger samt sanktioner. Det ville øge retssikkerheden for de registrerede og for de registeransvarlige.
140. Styrkelse af databeskyttelsesmyndighedernes uafhængighed, ressourcer og beføjelser bør kombineres med styrket samarbejde på multilateralt niveau, især i betragtning af det stigende antal databeskyttelsesproblemer på europæisk plan. Den hovedinfrastruktur, der skal anvendes i forbindelse med dette samarbejde, er tydeligvis Artikel 29-Gruppen.

### 10.2. Styrkelse af Artikel 29-Gruppens rolle

141. Historien viser, at fra Artikel 29-Gruppens start i 1997 og frem til i dag har gruppens funktionsmåde udviklet sig. Den er vokset til større uafhængighed og kan i praksis ikke længere kvalificere sig til blot at være en rådgivende gruppe under Kommissionen. EDPS plæderer for yderligere forbedringer af Artikel 29-Gruppens funktionsmåde, herunder dens infrastruktur og uafhængighed.
142. EDPS er af den opfattelse, at gruppens styrke reelt er forbundet med dens medlemmers uafhængighed og beføjelser. Artikel 29-Gruppens autonomi skal sikres i den nye retlige ramme i overensstemmelse med de kriterier, der er udviklet af EF-Domstolen i sag C-518/07 med henblik på databeskyttelsesmyndighedernes fulde uafhængighed. EDPS finder, at Artikel 29-Gruppen også skal have tilstrækkelige ressourcer og budgetmidler samt et styrket sekretariat, der skal understøtte gruppens arbejde.
143. Hvad angår Artikel 29-Gruppens sekretariat, værdsætter EDPS den kendsgerning, at det er integreret i databeskyttelsesorganet under GD for Retlige Anliggender med den fordel, at Artikel 29-Gruppen selv kan profitere af effektive og fleksible kontaktpersoner og opdaterede oplysninger om udviklingen på databeskyttelsesområdet. På den anden side sætter han spørgsmålstegn ved den kendsgerning, at Kommissionen (og mere specifikt databeskyttelsesorganet) på en og samme tid er medlem af, sekretariat for og modtager af Artikel 29-Gruppens udtalelser. Det kunne retfærdiggøre større uafhængighed til sekretariatet. EDPS opfordrer Kommissionen til at vurdere — i tæt samråd med interessenterne — hvordan denne uafhængighed bedst sikres.

<sup>(54)</sup> Sag C-518/07, *Kommissionen mod Tyskland*, endnu ikke offentliggjort i ECR.

<sup>(55)</sup> Se f.eks. artikel 43, stk. 2, i forordning (EF) nr. 45/2001, som indeholder sådanne krav til EDPS.

144. Endelig kræver en styrkelse af databeskyttelsesmyndighedernes beføjelser også stærkere beføjelser til Artikel 29-Gruppen med en struktur, der omfatter bedre regler og sikkerhedskontrol samt større gennemsigtighed. Denne vil blive udviklet til den rådgivende rolle samt til Artikel 29-Gruppens håndhævelsesrolle.

### 10.3. Styrkelse af Artikel 29-Gruppens rådgivende rolle

145. Artikel 29-Gruppens udtalelser skal gennemføres effektivt, når det handler om dens rådgivende rolle i forhold til Kommissionen, især i relation til fortolkningen og anvendelsen af principperne i direktivet og andre databeskyttelsesinstrumenter, med andre ord for at sikre den autoritative karakter af Artikel 29-Gruppens udtalelser. Yderligere drøftelser mellem databeskyttelsesmyndighederne er nødvendige med henblik på at identificere, hvordan dette kan inddrages i det retlige instrument.

146. EDPS anbefaler løsninger, der vil gøre udtalelser fra Artikel 29-Gruppen mere autoritative uden at ændre væsentligt ved dens funktionsmåde. EDPS foreslår at inddrage en forpligtelse for databeskyttelsesmyndighederne og Kommissionen til at tage nøje hensyn til erklæringer og fælles udtalelser vedtaget af Artikel 29-Gruppen, baseret på den model, der er vedtaget for udtalelser fra Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC)<sup>(56)</sup>. Derudover kunne det nye retlige instrument give Artikel 29-Gruppen den klare opgave at vedtage »fortolkende anbefalinger«. Disse alternative løsninger ville give udtalelserne fra Artikel 29-Gruppen en stærkere rolle, også ved domstolene.

### 10.4. Samordnet håndhævelse ved Artikel 29-Gruppen

147. I henhold til den nuværende ramme overlades håndhævelsen af databeskyttelseslovgivningen til 27 databeskyttelsesmyndigheder med kun lidt samordning med hensyn til håndteringen af specifikke sager. Når det drejer sig om sager, som involverer mere end en medlemsstat, eller som har en klar global dimension, mangedobler dette omkostningerne for virksomheder, der er tvunget til arbejde sammen med forskellige offentlige myndigheder i forbindelse med den samme aktivitet, og det øger risikoen for inkonsekvent anvendelse: i exceptionelle sager kan de samme behandlingsaktiviteter anses for at være lovlige af en databeskyttelsesmyndighed, mens de forbydes af en anden.

148. Nogle sager har en strategisk dimension, der skal tackles på en centraliseret måde. Artikel 29-Gruppen fremmer samordnings- og håndhævelsesforanstaltninger mellem

databeskyttelsesmyndighederne<sup>(57)</sup> i større databeskyttelsessspørgsmål med sådanne internationale konsekvenser. Det var tilfældet med sociale netværk og søgemaskiner<sup>(58)</sup> samt med hensyn til samordnede tilsyn, der blev udført i forskellige medlemsstater vedrørende telekommunikations- og sundhedssikringsspørgsmål.

149. Der er dog grænser for de håndhævelsesforanstaltninger, som Artikel 29-gruppen kan gennemføre i henhold til den nuværende ramme. Fælles holdninger kan indtages af Artikel 29-Gruppen, men der er ikke noget instrument til at sikre, at disse holdninger gennemføres effektivt i praksis.

150. EDPS foreslår at indsætte yderligere bestemmelser i det retlige instrument, der vil kunne støtte samordnet håndhævelse, herunder især:

— En forpligtelse til at sikre, at databeskyttelsesmyndighederne og Kommissionen tager nøje hensyn til erklæringer og fælles udtalelser vedtaget af Artikel 29-Gruppen<sup>(59)</sup>.

— En forpligtelse for databeskyttelsesmyndighederne til at samarbejde loyalt med hinanden, Kommissionen samt Artikel 29-Gruppen<sup>(60)</sup>. Som en praktisk illustration af et loyalt samarbejde kan der fastlægges en procedure, hvor databeskyttelsesmyndighederne informerer Kommissionen eller Artikel 29-Gruppen i tilfælde af nationale håndhævelsesforanstaltninger med et grænseoverskridende element, analogt med den procedure, der finder anvendelse i den nuværende ramme med hensyn til nationale afgørelser om tilstrækkelighed.

— Angivelse af afstemningsreglerne for at øge databeskyttelsesmyndighedernes forpligtelse til at gennemføre Artikel 29-Gruppens beslutninger. Man kunne f.eks. forestille sig, at Artikel 29-Gruppen påtænker at træffe afgørelse ved konsensus, og hvis konsensus ikke kunne opnås kun med kvalificeret flertal.

<sup>(56)</sup> Europa-Parlamentets og Rådets forordning (EF) nr. 1211/2009 af 25. november 2009 om oprettelse af Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC) og dens støttekontor, EUT L 337 af 18.12.2009, s. 1.

<sup>(57)</sup> Ud over Artikel 29-Gruppen etablerede den europæiske konference mellem datatilsynsmyndighederne for omkring 10 år siden en permanent workshop, der skal behandle grænseoverskridende klager på en samordnet måde. Selvom denne workshop udgør en ubestridelig merværdi med hensyn til dataudvekslingen mellem databeskyttelsesmyndighedernes ansatte og giver et pålideligt netværk af kontaktpunkter, kan det ikke anses for at være en samordningsmekanisme i forbindelse med beslutningstagning.

<sup>(58)</sup> Se breve fra Artikel 29-Gruppen af 12. maj 2010 og 26. maj 2010, offentliggjort på Artikel 29-Gruppens websted ([http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm)).

<sup>(59)</sup> Som ovenfor nævnt fastsættes en lignende forpligtelse i forordning (EF) nr. 1211/2009, der beskriver BERECs rolle (Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation).

<sup>(60)</sup> Se i den forbindelse artikel 3 i forordning (EF) nr. 1211/2009.

Derudover kunne en betragtning være, at de databeskyttelsesmyndigheder, der stemmer for vedtagelsen af et dokument, har en forpligtelse eller en politisk forpligtelse til at gennemføre den på nationalt niveau.

151. EDPS vil nedlægge protest mod indførelsen af mere effektive foranstaltninger, f.eks. at give udtalelser fra Artikel 29-Gruppen bindende virkning. Dette ville underminere de enkelte databeskyttelsesmyndigheders uafhængige status, som medlemsstater skal sikre i henhold til national lovgivning. Hvis Artikel 29-Gruppens afgørelser skal have en direkte indvirkning på tredjeparter såsom registeransvarlige, skal der fastlægges nye procedurer, herunder sikkerhedsregler såsom gennemsigtighed og søgsmålsadgang, herunder mulig appel ved EF-Domstolen.

#### 10.5. Samarbejde mellem EDPS og Artikel 29-Gruppen

152. Den måde, som EDPS og Artikel 29-Gruppen samarbejder på, vil også kunne finjusteres. EDPS er medlem af Artikel 29-Gruppen, og han bidrager inden for gruppen til udtalelser vedrørende de vigtigste strategiske udviklinger inden for EU, mens han sikrer sig sammenhæng med sine egne udtalelser. EDPS bemærker det stigende antal af emner vedrørende privatlivets fred, både i den private og offentlige sektor, som har konsekvenser på nationalt niveau i mange medlemsstater, og hvor Artikel 29-Gruppen har en særlig rolle at spille.
153. EDPS har en supplerende opgave med hensyn til at rådgive om udviklingen i EU-sammenhænge, som skal bevares. Som et europæisk organ udøver han denne rådgivende kompetence i forhold til EU's institutioner på den samme måde som nationale databeskyttelsesmyndigheder rådgiver deres regeringer.
154. EDPS og Artikel 29-Gruppen fungerer ud fra forskellige, men hinanden supplerende perspektiver. Der er således behov for at bevare og eventuelt forbedre samordningen mellem Artikel 29-Gruppen og EDPS med henblik på at sikre, at de arbejder sammen om de væsentligste databeskyttelsesemner, f.eks. ved at samordne dagsordener regelmæssigt<sup>(61)</sup>, og ved at sikre gennemsigtighed vedrørende emner, der har et mere nationalt eller specifikt EU-aspekt.
155. Samordning nævnes ikke i det nuværende direktiv af den simple årsag, at EDPS ikke eksisterede på det tidspunkt, hvor direktivet blev vedtaget, men efter at have eksisteret i seks år er komplementariteterne mellem EDPS og Artikel 29-Arbejdsgruppen synlige og vil kunne anerkendes formelt. EDPS minder om, at i henhold til forordning (EF) nr. 45/2001 er det hans opgave at samarbejde med de nationale databeskyttelsesmyndigheder og at deltage i Artikel 29-Gruppens aktiviteter. EDPS anbefaler

at nævne samarbejde eksplicit i det nye retlige instrument og at strukturere det, hvor det er nødvendigt, f.eks. ved at fastsætte en procedure for samarbejde.

#### 10.6. Samarbejde mellem EDPS og databeskyttelsesmyndighederne vedrørende tilsyn med EU's systemer

156. Disse overvejelser gælder også inden for områder, hvor tilsynet skal samordnes mellem det europæiske og nationale niveau. Dette er tilfældet for EU-organer, der behandler betydelige mængder af data, som modtages fra de nationale myndigheder eller for store informationssystemer med et europæisk og et nationalt element.
157. Det eksisterende system for nogle EU-organer og store informationssystemer — f.eks. Europol, Eurojust og den første generation af Schengeninformationssystemet (SIS) har fælles tilsynsorganer med repræsentanter fra de nationale databeskyttelsesmyndigheder — er et levn fra mellemstatsligt samarbejde i æraen før Lissabontraktaten og overholder ikke EU's institutionelle struktur, som Europol og Eurojust nu er en integreret del af, og hvori Schengen-reglerne nu også er blevet integreret<sup>(62)</sup>.
158. Af meddelelsen fremgår, at Kommissionen vil gennemføre en høring i 2011 af interessenterne vedrørende revisionen af disse tilsynssystemer. EDPS slår kraftigt til lyd for, at Kommissionen så hurtigt som muligt (inden for en kort og nærmere angivet tidsramme, se ovenfor) indtager en holdning i forbindelse med de igangværende drøftelser om tilsyn. Han indtager — i disse drøftelser — følgende standpunkt.
159. Som udgangspunkt skal det sikres, at alle tilsynsorganer opfylder de nødvendige kriterier for uafhængighed, ressourcer og håndhævelsesbeføjelser. Desuden skal det sikres, at der tages hensyn til de perspektiver og den ekspertise, som findes på EU-niveau. Det betyder, at der ikke alene skal finde samarbejde sted mellem de nationale myndigheder, men også med de europæiske databeskyttelsesmyndigheder (i øjeblikket EDPS). EDPS finder det nødvendigt at følge en model, som opfylder disse krav<sup>(63)</sup>.
160. I de senere år har man udviklet modellen for »samordnet tilsyn«. Denne tilsynsmodel, som den nu anvendes i Eurodac og i dele af toldinformationssystemet, udvides snart til visainformationssystemet (VIS) og den anden generation af Schengeninformationssystemet (SIS II). Modellen har 3 lag: 1) Tilsyn på nationalt niveau sikres af databeskyttelsesmyndighederne, 2) Tilsyn på EU-niveau sikres af EDPS; 3) Samordning sikres ved hjælp

<sup>(61)</sup> F.eks. på grundlag af listen over lovgivningsinitiativer, der offentliggøres én gang om året og opdateres regelmæssigt, og som findes på EDPS' websted.

<sup>(62)</sup> I henhold til forordning (EF) nr. 45/2001 har EDPS pligt til at samarbejde med disse organer.

<sup>(63)</sup> Hvad angår Eurojust, skal en model også tage hensyn til, at databeskyttelsestilsynet respekterer domstolens uafhængighed, i det omfang Eurojust behandler data i forbindelse med en strafferetssag.

af regelmæssige møder, som EDPS indkalder til, idet han fungerer som sekretariat for denne samordningsmekanisme. Modellen har vist sig at være en succes og effektiv og skal oprettes i fremtiden i forbindelse med andre informationssystemer.

## C. HVORDAN FORBEDRES ANVENDELSEN AF DEN NUVÆRENDE RAMME?

### 11. På kort sigt

161. Mens revurderingsprocessen er i gang, skal der gøres en indsats for at sikre fuld og effektiv gennemførelse af de nuværende regler. Disse regler vil stadig finde anvendelse, indtil den fremtidige ramme vedtages og derefter gennemføres i medlemsstaternes nationale lovgivninger. I den retning kan der identificeres flere aktionslinjer.
162. For det første skal Kommissionen fortsat overvåge medlemsstaternes overholdelse af direktiv 95/46/EF og, hvor det er nødvendigt, anvende sine beføjelser i henhold til EUF-traktatens artikel 258. For nylig er der blevet indledt en overtrædelsesprocedure for en fejl for korrekt at gennemføre artikel 28 i direktivet med hensyn til nødvendigheden af databeskyttelsesmyndighedernes uafhængighed<sup>(64)</sup>. Også på andre områder skal fuld overensstemmelse overvåges og håndhæves<sup>(65)</sup>. EDPS bifalder derfor Kommissionens forpligtelse og støtter den fuldt ud i meddelelsen om at forfølge en aktiv overtrædelsespolitik. Kommissionen skal også fortsætte den strukturelle dialog med medlemsstaterne om gennemførelse<sup>(66)</sup>.
163. For det andet skal håndhævelse på nationalt niveau fremmes for at sikre praktisk anvendelse af databeskyttelsesregler, herunder nye teknologiske fænomener og globale aktører. Databeskyttelsesmyndighederne skal gøre fuld brug af deres undersøgelses- og sanktionsbeføjelser. Det er også vigtigt, at de registreredes eksisterende rettigheder, navnlig adgangsretten, gennemføres fuldt ud i praksis.
164. For det tredje synes øget samordning af håndhævelsen at være nødvendig på kort sigt. Artikel 29-Gruppens rolle og dens fortolkende dokumenter i den forbindelse er afgørende, men også databeskyttelsesmyndighederne skal gøre deres yderste for at omsætte dem til praksis. Divergerende resultater i EU-sager eller globale sager skal undgås, og man skal nå frem til fælles fremgangsmåder inden for

Artikel 29-Gruppen. Samordnede undersøgelser i hele EU ved Artikel 29-Gruppen kan desuden tilføre væsentlig merværdi.

165. For det fjerde skal databeskyttelsesprincipper inkorporeres proaktivt i nye bestemmelser, der direkte eller indirekte kan have indvirkning på databeskyttelsen. På EU-niveau yder EDPS en stor indsats for at bidrage til bedre europæisk lovgivning, og disse bestræbelser skal også gøres på nationalt niveau. Databeskyttelsesmyndighederne skal derfor gøre fuld brug af deres rådgivende beføjelser for at sikre en proaktiv tilgang. Databeskyttelsesmyndigheder, herunder EDPS, kan også spille en proaktiv rolle i overvågningen af teknologiske udviklinger. Overvågning er vigtig for på et tidligt stade at kunne identificere nye tendenser, fremhæve mulige konsekvenser for databeskyttelsen, støtte databeskyttelsesvenlige løsninger og skabe større bevidsthed hos interessenterne.
166. Endelig skal yderligere samarbejde mellem de forskellige aktører på internationalt plan forfølges aktivt. Det er derfor vigtigt at styrke de internationale samarbejdsinstrumenter. Initiativer såsom Madridstandarderne og det igangværende arbejde i Europarådet og OECD fortjener fuld støtte. I den sammenhæng er det meget positivt, at US Federal Trade Commission nu også er blevet indlemmet i familien af datatilsynsmyndigheder inden for rammerne af deres internationale konference.

## D. KONKLUSIONER

### ALMINDELIGE BEMÆRKNINGER

167. EDPS hilser generelt Kommissionens meddelelse velkommen, da han er overbevist om, at en revurdering af den nuværende retlige ramme for databeskyttelse er nødvendig med henblik på at sikre effektiv beskyttelse i et globaliseret informationsfund under hastig udvikling.
168. Meddelelsen identificerer de væsentligste problemer og udfordringer. EDPS deler Kommissionens synspunkt om, at der også vil være behov for et stærkt databeskyttelses-system i fremtiden, som baseres på den opfattelse, at eksisterende generelle principper for databeskyttelse fortsat er gældende i et samfund, der gennemgår fundamentale forandringer. Som et resultat heraf efterlyser han en mere ambitiøs tilgang på en række punkter.
169. EDPS støtter fuldt ud den samlede tilgang til databeskyttelse. Han beklager imidlertid, at meddelelsen udelukker visse områder, f.eks. EU-institutioners og -organers behandling af personoplysninger, fra det generelle retlige instrument. Hvis Kommissionen skulle beslutte sig for at udelukke disse områder, opfordrer EDPS indtrængende

<sup>(64)</sup> Se sag C-518/07 og Kommissionens pressemeddelelse af 28. oktober 2010 (IP/10/1430).

<sup>(65)</sup> Kommissionen har indledt en overtrædelsesprocedure imod Det Forenede Kongerige for en påstået overtrædelse af forskellige databeskyttelsesbestemmelser, herunder kravet om fortrolighed i elektroniske meddelelser ved adfærdsbetinget reklamering. Se Kommissionens pressemeddelelse af 9. april 2009 (IP/09/570).

<sup>(66)</sup> Se i den sammenhæng Kommissionens første beretning om gennemførelsen af databeskyttelsesdirektivet, s. 22 ff.

Kommissionen til at vedtage et forslag om EU-niveaueu inden for den kortest mulige tidshorizont, men helst inden udgangen af 2011.

#### HOVEDPERSPEKTIVER

170. EDPS mener, at udgangspunktet for denne revurderingsproces bør være som følger:
- Databeskyttelsesordninger skal så vidt muligt snarere aktivt støtte end hindre andre legitime interesser (såsom den europæiske økonomi, personlig sikkerhed samt regeringers troværdighed).
  - De generelle principper for databeskyttelse skal og kan ikke ændres.
  - Yderligere harmonisering skal være et af hovedmålene med denne revurdering.
  - De grundlæggende rettigheder skal udgøre kernen i denne revurderingsproces. En grundlæggende rettighed sigter mod at beskytte borgere under alle omstændigheder.
  - Politi og retsvæsen skal inddrages i det nye retlige instrument.
  - Det nye retlige instrument skal formuleres på en teknologineutral måde.

#### ELEMENTER I EN NY RAMME

##### Harmonisering og forenkling

171. EDPS hilser Kommissionens tilsagn om at undersøge midlerne til at opnå yderligere harmonisering af databeskyttelsen på EU-niveau velkommen. EDPS fastlægger områder, hvor der er et presserende behov for yderligere og bedre harmonisering: definitioner, grunde til databehandling, registreredes rettigheder, internationale overførsler og databeskyttelsesmyndigheder.
172. EDPS foreslår at overveje følgende alternativer med henblik på at forenkle og/eller reducere omfanget af underretningskravene:
- Begrænse underretningsforpligtelsen for specifikke typer af behandlingsoperationer, som indebærer særlige risici.
  - En simpel registreringsforpligtelse for de registeransvarlige til at registrere (i modsætning til omfattende registrering af alle databehandlingsoperationer).
  - Indførelsen af en fælleseuropæisk standardformular til underretningen.
173. Ifølge EDPS er en forordning, et enkelt instrument, der er umiddelbart gældende i medlemsstaterne, den mest effektive måde at beskytte den grundlæggende ret til databe-

skyttelse og til at opnå yderligere konvergens i det indre marked.

#### Styrkelse af enkeltpersoners rettigheder

174. EDPS støtter meddelelsen med hensyn til at styrke enkeltpersoners rettigheder. Han stiller følgende forslag:
- Et princip om gennemsigtighed vil kunne indsættes i loven. Det er dog vigtigere at styrke de eksisterende bestemmelser, som omhandler gennemsigtighed (f.eks. den nuværende artikel 10 og 11 i direktiv 95/46/EF).
  - En bestemmelse vedrørende underretning om brud på datasikkerheden, som udvider den forpligtelse, der var indsat i det reviderede e-direktiv om privatlivets fred, fra visse udbydere til alle registeransvarlige, skal indsættes i det generelle instrument.
  - Grænserne for samtykke skal præciseres. En udvidelse af overførsler i tilfælde, hvor udtrykkeligt samtykke er påkrævet, bør overvejes samt vedtagelse af yderligere regler for online-miljøet.
  - Yderligere rettigheder bør indføres, f.eks. dataportabilitet og »retten til at blive glemt«, især i forbindelse med informations-samfundstjenester på internettet.
  - Børns interesser bør være bedre beskyttet med en række yderligere bestemmelser, der specifikt omhandler indsamlingen og yderligere behandling af børns personoplysninger.
  - Mekanismer for kollektiv søgsmålsadgang i forbindelse med brud på databeskyttelsesregler bør indføres i EU-lovgivningen med henblik på at bemyndige godkendte organer til at indlede søgsmål på vegne af grupper af enkeltpersoner.

#### Styrkelse af organisationernes/de registeransvarliges forpligtelser

175. Den nye ramme skal indeholde incitamenter for registeransvarlige til proaktivt at inddrage databeskyttelsesforanstaltninger i deres arbejdsgange. EDPS foreslår indførelsen af generelle bestemmelser om ansvarlighed og »privacy by design«. Der skal også indføres en bestemmelse om certificeringsordninger for privatlivets fred.

#### Globalisering og gældende lov

176. EDPS støtter det ambitiøse arbejde inden for rammerne af den internationale konference mellem datatilsynsmyndighederne med at udvikle de såkaldte Madridstandarder med henblik på at inkorporere dem i et bindende instrument og eventuelt afholde en regeringskonference. EDPS opfordrer Kommissionen til at tage konkrete skridt i den retning i tæt samarbejde med OECD og Europarådet.

177. Et nyt retligt instrument skal præcisere kriterierne for afgørelsen af, hvilken lovgivning der finder anvendelse. Det skal sikres, at data, der behandles uden for EU's grænser, ikke undslipper EU-lovgivningen, hvor der er et berettiget krav om anvendelse af samme. Hvis den retlige ramme ville have form af en forordning, ville der være identiske regler i alle medlemsstater, og det ville blive mindre relevant at afgøre, hvilken lov der finder anvendelse (inden for EU).
178. EDPS støtter fuldt ud målet om at sikre en mere fælles og sammenhængende tilgang i forhold til tredjelande og internationale organisationer. Bindende virksomhedsregler skal inddrages i det retlige instrument.

### Politi og retsvæsen

179. Ét samlet instrument, der omfatter politi og retsvæsen, kan åbne mulighed for særlige regler, der tager behørig hensyn til denne sektors specificiteter i overensstemmelse med erklæring 21, der er knyttet til Lissabontraktaten. Særlige sikkerhedsregler skal indføres for at kompensere de registrerede ved at give dem yderligere beskyttelse på et område, hvor der i sagens natur kan være større risiko for, at behandlingen af personoplysninger kan være krænkende.
180. Den nye retlige ramme skal så vidt muligt være klar, enkel og sammenhængende. En spredning af forskellige ordninger, som gælder for f.eks. Europol, Eurojust, SIS og Prüm, bør undgås. EDPS er klar over, at en ensretning af reglerne fra de forskellige systemer skal foretages omhyggeligt og gradvist.

### Databeskyttelsesmyndigheder og samarbejdet mellem databeskyttelsesmyndigheder

181. EDPS støtter fuldt ud Kommissionens mål om at behandle spørgsmålet om databeskyttelsesmyndighedernes status og styrke deres uafhængighed, ressourcer og håndhævelsesbeføjelser. Han anbefaler:
- at udtrykket »databeskyttelsesmyndighedernes uafhængighed« kodificeres i det nye retlige instrument, som angivet af EF-Domstolen.
  - at det i loven anføres, at databeskyttelsesmyndigheder skal have tilstrækkelige ressourcer.
  - at give myndigheder harmoniserede undersøgelses- og sanktionsbeføjelser.

182. EDPS plæderer for yderligere forbedringer af Artikel 29-Gruppens funktionsmåde, herunder dens uafhængighed og infrastruktur. Desuden skal gruppen have stillet tilstrækkelige ressourcer til rådighed og styrket sin sekretariatsfunktion.

183. EDPS foreslår at styrke gruppens rådgivende rolle ved at indføre en forpligtelse for databeskyttelsesmyndighederne og Kommissionen til at *tage nøje hensyn til udtalelser og fælles holdninger*, der er vedtaget af gruppen. EDPS bifalder ikke, at udtalelser fra Artikel 29-Gruppen skal have bindende virkning, navnlig på grund af de enkelte databeskyttelsesmyndigheders uafhængige status. EDPS anbefaler, at Kommissionen indfører særlige bestemmelser for at øge samarbejdet med EDPS inden for det nye retlige instrument.

184. EDPS råder på det kraftigste Kommissionen til så hurtigt som muligt at tage stilling til spørgsmålet om tilsyn med EU's organer og store informationssystemer, idet der tages hensyn til, at alle tilsynsorganer skal opfylde de nødvendige uafhængighedskriterier, have tilstrækkelige ressourcer og håndhævelsesbeføjelser, og at det sikres, at EU-perspektivet er velrepræsenteret. EDPS støtter modellen for »samordnet tilsyn«.

*Forbedringer under det nuværende system:*

185. EDPS opfordrer Kommissionen til:
- at fortsætte overvågningen af medlemsstaternes overholdelse af direktiv 95/46/EF og, hvor det er nødvendigt, anvende sine håndhævelsesbeføjelser i henhold til EUF-traktatens artikel 258.
  - at fremme håndhævelsen på nationalt niveau og samordningen af håndhævelsen.
  - at inkorporere databeskyttelsesprincipper proaktivt i nye bestemmelser, der kan have indvirkning på, direkte eller indirekte, databeskyttelsen.
  - aktivt at forfølge yderligere samarbejde mellem de forskellige aktører på internationalt niveau.

Udfærdiget i Bruxelles, den 14. januar 2011.

Peter HUSTINX  
Tilsynsførende for Databeskyttelse