Europaudvalget 2010
KOM (2010) 0609
Offentligt

EUROPA-KOMMISSIONEN

Bruxelles, den 4.11.2010
KOM(2010) 609 endelig

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

En global metode til beskyttelse af personoplysninger i Den Europæiske Union

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

En global metode til beskyttelse af personoplysninger i Den Europæiske Union

1. NYE UDFORDRINGER I BESKYTTELSEN AF PERSONOPLYSNINGER

Med databeskyttelsesdirektivet[1] fra 1995 blev der sat en historisk milesten i beskyttelsen af personoplysninger i Den Europæiske Union. Direktivet afspejler to af det europæiske integrationsprojekts ældste ambitioner, som begge er af stor vigtighed: På den ene side beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, særlig den grundlæggende ret til databeskyttelse, på den anden side dannelsen af det indre marked med fri udveksling af personoplysninger.

Nu femten år senere er dette dobbelte mål stadig aktuelt og direktivets principper stadig velbegrundede. **Imidlertid har den hastige teknologiske udvikling og globaliseringen grundlæggende ændret den verden, vi lever i, og skabt nye udfordringer for beskyttelsen af personoplysninger.**

Med nutidens teknologi er folk let i stand til at udveksle oplysninger om deres adfærd og præferencer og gøre dem offentligt tilgængelige for andre over alt i verden i et hidtil uset omfang. Sociale netværkssteder med flere hundrede millioner medlemmer over hele verden er måske det tydeligste, om end ikke det eneste, eksempel på dette fænomen. "Cloud computing", hvor applikationer, fælles ressourcer og oplysninger befinder sig på en fjernserver ("i skyen") og leveres via internettet kan ligeledes vise sig at være en udfordring for databeskyttelsen, fordi fysiske personer kan miste kontrollen over potentielt følsomme oplysninger, når de gemmer oplysninger via programmer, som er lagret på andres hardware. En nylig undersøgelse bekræftede, at databeskyttelsesmyndigheder, erhvervssammenslutninger og forbrugerorganisationer sammenstemmende synes at være af den opfattelse, at truslerne fra internetaktiviteter mod privatlivets fred og mod beskyttelsen af personoplysninger er stigende[2].

Samtidig er **måderne, hvor personoplysninger indsamles, blevet mere og mere sofistikerede og vanskeligere at opdage.** Eksempelvis kan erhvervsdrivende nu målrette deres indsats mod enkeltpersoner ud fra de oplysninger, de indsamler om disse personers adfærd ved hjælp af avancerede redskaber. Hertil kommer, at den stigende anvendelse af procedurer, der muliggør automatisk dataindsamling, såsom e-billetter, opkrævning af vejafgifter og udstyr til geografisk sporing, gør det lettere at spore, hvor enkeltpersoner, der benytter mobilt udstyr, befinder sig Offentlige myndigheder anvender ligeledes flere og flere personoplysninger til forskellige formål såsom sporing af enkeltindivider ved udbrud af overførbare sygdomme, mere effektiv forebyggelse og bekæmpelse af terrorisme og

---

1 Europa-Parlamentets og Rådets direktiv 95/46/EF af 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

2 Se *Study on the economic benefits of privacy enhancing technologies* (undersøgelse af de økonomiske fordele ved teknologier til beskyttelse af privatlivets fred), http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf, s. 14.

kriminalitet, forvaltning af socialsikringsordninger, skattemæssige formål og som led i deres digitale forvaltning.

Alt dette må nødvendigvis rejse spørgsmålet om, hvorvidt den eksisterende EU-databeskyttelseslovgivning er tilstrækkelig effektiv til at håndtere disse udfordringer fuldt ud.

Derfor indledte Kommissionen en revision af den eksisterende EU-lovgivning med en konference på højt plan i maj 2009 efterfulgt af en offentlig høring, der løb indtil udgangen af 2009[3]. Desuden blev der iværksat en række undersøgelser[4].

Resultaterne bekræftede, at principperne i direktivet stadig er velbegrundede, og at dets teknologineutrale karakter skal fastholdes. Gennemgangen viste, at der på flere områder er problemer og specifikke udfordringer. De omfatter:

- *Håndtering af konsekvenserne af ny teknologi*

Høringssvarene fra både privatpersoner og organisationer bekræftede, at det er nødvendigt at klarlægge og præcisere, hvordan databeskyttelsesprincipperne skal anvendes på ny teknologi, således at det sikres, at personoplysninger rent faktisk beskyttes effektivt, uanset hvilken teknologi der anvendes ved databehandlingen, og at de registeransvarlige er fuldt ud bevidste om, hvilke konsekvenser ny teknologi har for databeskyttelse. Det er der til dels taget hånd om i direktiv 2002/58/EF (det såkaldte "e-databeskyttelsesdirektiv")[5], som supplerer det mere generelle databeskyttelsesdirektiv og specifikt omhandler telesektoren[6].

- *Større vægt på databeskyttelse som led i det indre marked*

Hvis der noget, som interessenter, ikke mindst multinationale virksomheder, har udtrykt bekymring over igen og igen, er det den utilstrækkelige harmonisering af medlemsstaternes lovgivning om databeskyttelse, selv om den fælles EU-lovgivning er på plads. De

---

3 Høringssvarene på Kommissionens offentlige høring kan ses på: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Mere målrettede interessenthøringer blev afholdt i 2010. Næstformand for Kommissionen Viviane Reding var vært ved et møde på højt niveau med interessenterne den 5. oktober 2010 i Bruxelles. Kommissionen rådførte sig desuden med artikel 29-gruppen, som ydede et omfattende bidrag til høringen i 2009 (WP 168) og vedtog en særskilt udtalelse i juli 2010 om princippet om ansvarlighed (WP 173).

4 Ud over undersøgelsen de økonomiske fordele ved teknologier til beskyttelse af privatlivets fred (jf. fodnote 2) henvises til Comparative Study on Different Approaches to New Privacy Challenges, in particular in the Light of Technological Developments (sammenlignende undersøgelse af forskellige tilgange til de nye udfordringer for privatlivets fred, særlig i lyset af den teknologiske udvikling) fra januar 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). I øjeblikket arbejdes der på en konsekvensanalyse af den kommende EU-lovgivning om beskyttelse af personoplysninger.

5 Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12 juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

6 Databeskyttelsesdirektivet 95/46/EF af 24. oktober 1995 fastsætter databeskyttelsesstandarder for alle EU-retsakter, herunder for e-databeskyttelsesdirektivet (direktiv 2002/58/EF, som ændret ved direktiv 2009/136/EF), EUT L 337 af 18.12.2009, s. 11). E-databeskyttelsesdirektivet finder anvendelse på behandling af personoplysninger i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet. I direktivet omsættes principperne i databeskyttelsesdirektivet til specifikke regler for telesektoren. Direktiv 95/46/EF anvendes på ikke-offentlige kommunikationstjenester.

understreger behovet for øget retssikkerhed, færre administrative byrder og lige vilkår for erhvervsdrivende og andre registeransvarlige.

- *Håndtering af globaliseringen og forbedring af internationale dataoverførsler*

Mange interessenter fremhæver, at den stigende outsourcing af databehandling ofte til lande uden for EU er forbundet med flere problemer. Hvilke regler om behandling finder anvendelse, og hvem bærer egentlig ansvaret? For så vidt angår internationale dataoverførsler fandt mange organisationer, at de nuværende ordninger ikke er fuldt ud tilfredsstillende, men trænger til at blive underkastet en revision og gjort mere strømlinede, således at dataoverførsler bliver enklere og mindre besværlige.

- *En bedre institutionel ordning til effektiv håndhævelse af databeskyttelsesreglerne*

Blandt interessenterne er der enighed om, at databeskyttelsesmyndighederne skal spille en vigtigere rolle med henblik på at forbedre håndhævelsen af databeskyttelsesreglerne. Derudover efterlyste nogle organisationer større gennemsigtighed i artikel 29-gruppens arbejde (se nedenfor under 2.5.) og en nærmere præcisering af dens opgaver og beføjelser.

- *Øget sammenhæng i retsreglerne om databeskyttelse*

I forbindelse med den offentlige høring understregede samtlige interessenter nødvendigheden af et overordnet instrument, der finder anvendelse på databehandlingsprocesser i alle sektorer og på alle politiske områder i EU, således at der skabes en integreret metode og opnås en beskyttelse, der er ensartet, konsekvent og effektiv[7].

Hvis EU skal kunne håndtere ovenstående udfordringer, skal der **udvikles en global og sammenhængende metode, der kan sikre, at retten til beskyttelse af personoplysninger respekteres både i og uden for EU**. Med Lissabontraktaten fik EU flere midler til rådighed til at nå dette mål. EU's charter om grundlæggende rettigheder, hvis artikel 8 anerkender en selvstændig ret til beskyttelse af personoplysninger, er blevet retligt bindende, og der er indført et nyt retsgrundlag[8], hvorved vejen er banet for en global og sammenhængende EU-lovgivning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Særlig udstyrer det nye retsgrundlag EU med ét samlet retligt instrument til regulering af databeskyttelsen, herunder på områderne politisamarbejde og retligt samarbejde i straffesager. Den fælles udenrigs- og sikkerhedspolitik er derimod kun delvis omfattet af artikel 16 i traktaten om Den Europæiske Unions funktionsmåde, idet specifikke regler for medlemsstaternes databehandling skal fastsættes ved Rådets afgørelse på et andet retsgrundlag[9].

På grundlag af disse nye juridiske muligheder kan og vil Kommissionen give det højeste prioritet at sikre, at den grundlæggende ret til databeskyttelse respekteres i hele EU og i alle sine politikker, men samtidig lægge større vægt på databeskyttelse som led i det indre marked og lette den frie udveksling af personoplysninger. I den forbindelse må det ikke på nogen

---

7 I særskilte bemærkninger, som blev fremsat efter den offentlige høring, anmodede Europol og Eurojust indtrængende om, at der ikke desto mindre blev taget hensyn til den særlige karakter af deres arbejde med hensyn til koordinering af retshåndhævelse og kriminalitetsforebyggelse.

8 Se artikel 16 i traktaten om Den Europæiske Unions funktionsmåde.

9 Se artikel 16, stk. 2, sidste afsnit, i traktaten om den Europæiske Unions funktionsmåde og artikel 39 i traktaten om Den Europæiske Union.

måde ske på bekostning af andre af chartrets grundlæggende rettigheder eller andre af traktaternes mål.

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, således at man fortsat kan sikre fysiske personer et højt beskyttelsesniveau med hensyn til behandling af personoplysninger på alle de områder, hvor EU agerer. Dermed kan EU bevare sin ledende rolle i arbejdet for at udbrede høje databeskyttelsesstandarder i hele verden.

2. HOVEDFORMÅL MED DEN GLOBALE METODE TIL DATABESKYTTELSE

2.1. Styrkelse af fysiske personers rettigheder

2.1.1. Fysiske personer skal nyde passende beskyttelse i enhver situation

Målet med reglerne i de nuværende EU-databeskyttelsesinstrumenter er at beskytte fysiske personers grundlæggende rettigheder, herunder særlig deres ret til beskyttelse af personoplysninger, i overensstemmelse med EU's charter om grundlæggende rettigheder[10].

Begrebet "personoplysninger" er et af nøglebegreberne i beskyttelsen af fysiske personer i de nuværende EU-databeskyttelsesinstrumenter og medfører, at registeransvarlige og registerførere pålægges forskellige forpligtelser[11]. "Personoplysninger" er defineret, så begrebet dækker alle oplysninger, der direkte eller indirekte vedrører en identificeret eller en identificerbar person. Til bestemmelse af, om en person er identificerbar, bør alle de midler tages i betragtning, der inden for rimelighedens grænser vil kunne benyttes af enten den registeransvarlige eller enhver anden person til at identificere den pågældende person[12]. EU-lovgiveren har bevidst valgt denne metode, da den er fleksibel og derfor kan anvendes i forskellige situationer og ved forskellige ændringer, der påvirker de grundlæggende rettigheder, herunder de, der ikke kunne forudses, da direktivet blev vedtaget. Konsekvensen af en så bredt anlagt og fleksibel metode er imidlertid, at det i mange tilfælde ikke står klart, hvilken tilgang der skal vælges, om fysiske personer rent faktisk nyder databeskyttelsesrettigheder, og om registeransvarlige skal overholde direktivets krav[13].

I nogle situationer kræver behandling af specifikke oplysninger yderligere foranstaltninger i henhold til EU-retten. Sådanne foranstaltninger findes allerede i visse tilfælde. Eksempelvis er lagring af data i terminaludstyr (f.eks. mobiltelefoner) kun tilladt på betingelse af, at den fysiske person har givet sit samtykke. Muligvis er det også nødvendigt at tage dette op på EU-niveau med hensyn til eksempelvis oplysninger med nøglekode, lokaliseringsdata og "data

---

[10] Se Den Europæiske Unions Domstol, sag C-101/01, Bodil Lindqvist, Sml. 2003 I, s. 2097, 96, 97 og sag C-275/06, Productores de Música de España (Promusicae) mod Telefónica de España SAU, Sml. 2008 I, s. 271. Se også Den Europæiske Menneskerettighedsdomstols retspraksis eksempelvis i sagerne: S. og Marper mod Det Forenede Kongerige, 4.12. 2008 (klage nr. 30562/04 og 30566/04) og Rotaru mod Rumænien, 4.5. 2000, (klage nr. 28341/95, præmis 55, ECHR 2000-V.

[11] Se definitionen af "registeransvarlig" og "registerfører" i artikel 2, litra d) og e), i direktiv 95/45/EF.

[12] Se betragtning 26 til direktiv 95/46/EF.

[13] Se eksempelvis den sagen om IP-adresser, som analyseres i artikel 29-gruppens udtalelse 4/2007 om begrebet personoplysninger (WP 136).

mining"-teknologier, hvor data fra forskellige kilder kan kombineres, eller i tilfælde hvor det er nødvendigt at sikre fortroligheden og integriteten i informationsteknologiske systemer[14].

Alle de ovennævnte problemstillinger bør undersøges grundigt.

Kommissionen vil overveje, **hvordan man kan sikre, at databeskyttelsesreglerne anvendes på sammenhængende vis, under hensyntagen til den nye teknologis indvirkning på fysiske personers rettigheder og frihedsrettigheder og målet om at sikre fri udveksling af personoplysninger i det indre marked**.

2.1.2. Øget gennemsigtighed for de registrerede

Gennemsigtighed er en grundlæggende betingelse for, at fysiske personer kan have kontrol over og beskytte deres egne personoplysninger. Derfor er det afgørende, at de registeransvarlige **informerer fysiske personer åbent, klart og tydeligt** om, hvordan deres personoplysninger indsamles og behandles, hvorfor de indsamles, hvor lang tid de lagres, og hvilke rettigheder de som personer har, hvis de ønsker at få adgang til, berigtige eller slette oplysningerne. De relevante bestemmelser om information af den registrerede[15] er utilstrækkelige.

Kravet om, at det skal være **let at finde frem til oplysninger, at oplysningerne er lette at forstå, og at sprogbrugen er klar og enkel** er et grundlæggende element i gennemsigtighed. Dette er særlig relevant på internettet, hvor erklæringer om beskyttelse af personoplysninger ofte viser sig at være uklare og vanskelige at finde frem til, uigennemsigtige[16] og ikke altid helt i overensstemmelse med gældende regler. Der ses hyppigt eksempler herpå inden for adfærdsbaseret annoncering på internettet, hvor såvel den store vækst i udbydere af adfærdsbaseret annoncering som kompleksiteten af den anvendte teknologi gør det vanskeligt for den enkelte at vide, hvem der indsamler hvilke oplysninger med hvilket formål.

I den forbindelse **bør** børn nyde særlig beskyttelse, eftersom de ofte er mindre bevidste om risici, konsekvenser, forholdsregler og rettigheder for så vidt angår behandling af personoplysninger[17].

Kommissionen vil overveje:

- at indføre **et generelt princip om gennemsigtighed i behandlingen** af personoplysninger i EU-lovgivningen

- at pålægge registeransvarlige **specifikke forpligtelser**, herunder over for børn, med hensyn til hvilke informationer de skal give og på hvilken måde disse skal gives

---

14 Se eksempelvis den tyske forfatningsdomstols (Bundesverfassungsgericht) dom af 27. februar 2008, 1 BvR 370/07.

15 Se artikel 10 og 11 i direktiv 95/46/EF.

16 En Eurobarometerundersøgelse fra 2009 viste, at ca. halvdelen af respondenterne mente, at meddelelser om beskyttelse af privatlivets fred på websites var "meget uklare" eller "temmelig uklare" (se Flash Eurobarometer nr. 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Se den kvalitative undersøgelse Safer Internet for Children (et sikrere internet for børn), der omhandler børn på henholdsvis 9-10 år og 12-14 år. Undersøgelsen viser, at børn har tendens til at undervurdere de risici, der knytter sig til anvendelse af internettet og bagatellisere konsekvenserne af deres risikoadfærd (kan hentes på: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

- at udfærdige en eller flere **EU-standardformularer** ("**erklæringer om beskyttelse af personoplysninger**"), som skal anvendes af registeransvarlige.

Det er ligeledes vigtigt for fysiske personer at modtage information, når deres personoplysninger af vanvare eller på ulovlig vis ødelægges, går tabt, ændres eller videregives til uautoriserede personer. Ved den nylige ajourføring af e-databeskyttelsesdirektivet indførtes en **obligatorisk underretningspligt ved persondatasikkerhedsbrud**, der dog udelukkende dækker telesektoren. Eftersom risikoen for datasikkerhedsbrud også er til stede i andre sektorer (såsom den finansielle sektor) vil Kommissionen undersøge, hvordan pligten til at underrette om persondatasikkerhedsbrud kan udbredes til også at omfatte andre sektorer i overensstemmelse med Kommissionens erklæring til Europa-Parlamentet om datasikkerhedsbrud, som Kommissionen afgav i 2009 i forbindelse med reformen af de relevante retsregler for elektroniske kommunikationsnet og –tjenester[18]. Undersøgelserne griber ikke ind i e-databeskyttelsesdirektivets bestemmelser, som skal være gennemført i national lovgivning senest den 25. maj 2011[19]. Det er vigtigt at sikre en konsekvent og sammenhængende tilgang på området.

Kommissionen vil:

- undersøge, hvordan der i de generelle retsregler kan indføres en **generel underretningspligt ved persondatasikkerhedsbrud**, herunder hvem der skal underrettes, og kriterierne for hvornår underretningspligten indtræder.

2.1.3. Øget kontrol over egne personoplysninger

To vigtige forudsætninger skal være opfyldt, for at fysiske personer kan nyde et højt databeskyttelsesniveau: **At registerførere udelukkende behandler de data, der ud fra formålet er nødvendige (dataminimering), og at de registrerede reelt har kontrol over deres egne personoplysninger**. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf, jf. artikel 8, stk. 2, i EU's charter om grundlæggende rettigheder. Fysiske personer bør altid have mulighed for at få adgang til, berigtige, slette eller blokere deres personoplysninger, undtagen i tilfælde hvor der i medfør af loven er gyldige grunde til at forhindre det. Det er rettigheder, der allerede findes i de nuværende retsregler. Den måde, som rettighederne kan udøves på, varierer, og derfor er de i praksis vanskeligere at udøve i nogle medlemsstater end i andre. Hertil kommer, at det er blevet særlig vanskeligt på internettet, hvor data ofte opbevares, uden at den berørte person bliver informeret og/eller har givet sit samtykke.

I den forbindelse er det særligt relevant at nævne sociale netværkssteder, hvor det er meget vanskeligt for fysiske personer at have kontrol over deres personoplysninger. Kommissionen

---

[18] "Kommissionen noterer sig, at Europa-Parlamentet og Rådet ønsker, at pligten til at underrette om brud på persondatasikkerheden ikke kun skal gælde i sektoren for elektronisk kommunikation, men også eksempelvis for udbydere af informationssamfundstjenester […]. Kommissionen vil derfor straks tage fat på de fornødne forberedelser, herunder høring af interesseparter, for i givet fald at kunne fremlægge forslag på dette område ved udgangen af 2011[…]", som kan hentes på: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//DA. Se endvidere betragtning 59 i direktiv 2009/136/EF, der ændrer e-databeskyttelsesdirektivet (direktiv 2002/58/EF). "Det forhold, at det helt generelt er i brugernes interesse at blive underrettet, gælder naturligvis ikke kun den elektroniske kommunikationssektor, og der bør derfor på fællesskabsplan som en prioritering indføres udtrykkelige, obligatoriske krav om underretning i alle sektorer."

[19] Artikel 4 i direktiv 2009/136/EF.

har modtaget forskellige forespørgsler fra personer, som ikke har haft mulighed for at hente de personlige oplysninger, som tjenesteudbydere på internettet ligger inde med om de pågældende, f.eks. fotos af dem, og som med andre ord er blevet forhindret i at udøve deres ret til adgang, berigtigelse og sletning.

Sådanne rettigheder bør derfor tydeliggøres, præciseres og muligvis også styrkes.

Kommissionen vil derfor undersøge:

– hvordan **princippet om dataminimering** kan styrkes

– hvordan man kan **give bedre muligheder** for, at fysiske personer **rent faktisk kan udøve deres ret til adgang, berigtigelse, sletning og blokering af personoplysninger** (f.eks. ved at indføre frister for svar på anmodninger herom, ved at tillade, at rettigheder kan udøves via internettet eller ved at knæsætte princippet om, at adgang til personoplysninger skal være gratis

– hvordan man kan tydeliggøre den såkaldte "**ret til at blive glemt**", dvs. fysiske personers ret til at få slettet personoplysninger, så de ikke længere kan databehandles, når de ikke længere er nødvendige til legitime formål. Det er eksempelvis tilfældet, når databehandlingen er betinget af den fysiske persons samtykke, når vedkommende trækker sit samtykke tilbage, eller når lagringsperioden er udløbet

- hvordan de registreredes rettigheder kan udbygges ved at sikre "**dataportabilitet**", dvs. fysiske personers udtrykkelige ret til at fjerne egne personoplysninger (eksempelvis fotos eller en liste over venner) fra et program eller tjeneste og derefter, så vidt det er teknisk muligt, portere dem til et andet program eller tjeneste, uden at registeransvarligere kan modsætte sig det.

2.1.4. Oplysningsarbejde

Gennemsigtighed er afgørende, men derudover er der også behov for at oplyse offentligheden og særlig unge bedre om, hvilke risici der knytter sig til behandling af personoplysninger, og hvilke rettigheder de har. Eurobarometerundersøgelse fra 2008 viste, at de allerfleste EU-borgere er af den opfattelse, at bevidstheden om beskyttelse af personoplysninger i deres eget land er meget begrænset[20]. Derfor bør en bred vifte af aktører iværksætte og støtte oplysningsaktiviteter, f.eks. medlemsstaternes myndigheder, herunder særlig databeskyttelsesmyndigheder og uddannelsesinstitutioner, samt registeransvarlige og organisationer i civilsamfundet. Herunder bør der iværksættes foranstaltninger af ikke-lovgivningsmæssig art såsom oplysningskampagner i skrevne og elektroniske medier samt klar information på internettet, som tydeligt beskriver, hvilke rettigheder de registrerede har, og hvilke forpligtelser der påhviler de registeransvarlige.

Kommissionen vil undersøge:

– om det er muligt at **medfinansiere oplysningsaktiviteter** via EU's budget

– om der er behov og mulighed for i lovgivningen at indføje **en forpligtelse til oplysningsaktiviteter** på dette område.

[20] Se Flash Eurobarometer 225 – Data Protection in the European Union (Databeskyttelse i Den Europæiske Union): http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

2.1.5. Sikring af informeret og frivilligt samtykke

I de gældende regler hedder det, at når der kræves informeret samtykke, skal den fysiske persons samtykke til behandling af vedkommendes personoplysning være en "frivillig, specifik og informeret viljetilkendegivelse" af vedkommendes ønsker, hvorved vedkommende indvilliger i databehandlingen[21]. Dette krav fortolkes imidlertid forskelligt i medlemsstaterne; i nogle kræves der altid skriftligt samtykke, i andre accepteres underforstået samtykke.

Desuden er det på internettet oftest vanskeligere for fysiske personer at få klarhed over deres rettigheder og give informeret samtykke, fordi det er uklart hvilken politik for beskyttelse af privatlivets fred der følges. Og det er endnu mere indviklet i de tilfælde, hvor det end ikke står klart, hvad der forstås ved frivillig, specifik og informeret samtykke til databehandling. Det gælder f.eks. ved adfærdsbaseret annoncering, hvor bestemte browserindstillinger af nogle betragtes som udtryk for brugerens samtykke og af andre ikke gør det.

Der bør derfor ske en afklaring af bestemmelserne vedrørende den registreredes samtykke med henblik på at sikre, at der gives **informeret samtykke**, og at den fysiske person er helt klar over, at vedkommende giver samtykke, og over, hvilken databehandling vedkommende giver samtykke til, i overensstemmelse med artikel 8 i EU's charter om grundlæggende rettigheder. Klare nøglebegreber kan ligeledes fremme udviklingen af selvregulerende foranstaltninger med henblik på at finde frem til praktiske løsninger, der er i overensstemmelse med EU-retten.

Kommissionen vil undersøge, hvordan **reglerne om samtykke kan tydeliggøres og styrkes**.

2.1.6. Beskyttelse af følsomme oplysninger

Behandling af følsomme personlige oplysninger, dvs. personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssigt tilhørsforhold samt behandling af oplysninger om helbredsforhold eller seksuelle forhold er som hovedregel forbudt. Der er få undtagelser, og visse betingelser skal da være opfyldt og visse sikkerhedsforanstaltninger være truffet[22]. I lyset af den teknologiske udvikling og andre udviklingstendenser i samfundet er der imidlertid behov for at tage de gældende bestemmelser om følsomme oplysninger op til fornyet overvejelse, at undersøge, om nogle datakategorier bør tilføjes, og at afklare, under hvilke betingelser de kan behandles. Det angår eksempelvis genetiske data, som på nuværende tidspunkt ikke nævnes eksplicit som en kategori af følsomme oplysninger.

Kommissionen vil overveje:

– om andre kategorier af oplysninger bør betragtes som "**følsomme oplysninger**", f.eks. genetiske data

– yderligere at afklare og harmonisere betingelserne for at tillade behandling af kategorier af følsomme oplysninger.

---

21 Jf. artikel 2, litra h), i direktiv 95/46/EF.

22 Jf. artikel 8 i direktiv 95/46/EF.

2.1.7. Mere effektive retsmidler og sanktioner

En vigtig forudsætning for at kunne håndhæve databeskyttelsesreglerne er **effektive bestemmelser om retsmidler og sanktioner**. Mange sager, hvor en fysisk person berøres af en overtrædelse af databeskyttelsesreglerne, berører ligeledes en lang række andre fysiske personer i en lignende situation.

Derfor vil Kommissionen:

– overveje at give databeskyttelsesmyndigheder, organisationer i civilsamfundet og **andre organisationer, der repræsenterer de registreredes interesser**, **mulighed for at anlægge sag ved de nationale domstole**

– vurdere behovet for at **styrke de gældende bestemmelser om sanktioner**, f.eks. ved at operere eksplicit med strafferetlige sanktioner i tilfælde af alvorlige krænkelser af databeskyttelsen, for at gøre bestemmelserne mere effektive.

2.2. Større vægt på databeskyttelse som led i det indre marked

2.2.1. Styrket retssikkerhed og lige vilkår for registeransvarlige

Databeskyttelse i EU har en **tydelig forbindelse til det indre marked**, nemlig når det gælder behovet for at sikre fri udveksling af personoplysninger mellem medlemsstaterne. Følgelig er direktivets harmonisering af de nationale databeskyttelseslove ikke begrænset til en minimumsharmonisering, men fører til en harmonisering, der i princippet er fuldstændig[23].

Samtidig indrømmer direktivet dog medlemsstaterne et vist råderum på visse områder og tillader dem at opretholde eller indføre særlige ordninger med henblik på specifikke tilfælde[24]. Dette har – sammen med medlemsstaternes til tider fejlagtige gennemførelse af direktivet – ført til forskelle mellem de nationale love, der gennemfører direktivet. Disse **forskelle modarbejder et af direktivets hovedformål, nemlig at sikre den frie udveksling af personoplysninger i det indre marked.** Det gælder en lang række sektorer og i mange sammenhænge, eksempelvis ved behandling af personoplysninger ved ansættelsesforhold og til brug i den offentlige sundhedssektor. Den manglende harmonisering udgør et af de tilbagevendende problemer, som private interessenter, særligt erhvervsdrivende, fremhæver som de væsentligste. Den indebærer nemlig ekstraomkostninger og administrative byrder for dem. Det er ikke mindst tilfældet for registeransvarlige, der opererer i mere end en medlemsstat. Disse registeransvarlige er tvunget til at overholde krav og praksis, der gælder i hvert af de pågældende lande. Desuden skaber forskellene i medlemsstaternes gennemførelse af direktivet manglende retssikkerhed, ikke blot for de registeransvarlige, men også for de registrerede, idet der opstår risiko for fordrejning af det ensartede beskyttelsesniveau, som direktivet forventes at skabe og sikre.

Kommissionen vil undersøge, hvordan der kan opnås **yderligere harmonisering af databeskyttelsesreglerne på EU-niveau**.

---

[23] Den Europæiske Unions Domstol, sag C-101/01, Bodil Lindqvist, Sml. 2003 I, s. 2097, 96, 97.

[24] *Ibidem*, 97. Se også betragtning 9 i direktiv 95/46/EF.

2.2.2. Færre administrative byrder

Ved at etablere lige konkurrencevilkår mindskes behovet for at opfylde de forskellige nationale krav, og dermed lettes de registeransvarliges administrative byrder. Et andet konkret skridt, der kan lette de administrative byrder og reducere de registeransvarliges omkostninger, kunne bestå i **en ajourføring og forenkling af det nuværende anmeldelsessystem**[25]. Der hersker almindelig enighed blandt de registeransvarlige om, at den nugældende forpligtelse til at underrette databeskyttelsesmyndighederne om alle databehandlingsaktiviteter er en temmelig byrdefuld forpligtelse, som ikke i sig selv skaber nogen merværdi i forhold til beskyttelsen af fysiske personers personoplysninger. Desuden er der her tale om et af de tilfælde, hvor direktivet indrømmer medlemsstaterne et vist råderum, idet de har mulighed for at vedtage mulige undtagelser og forenklinger, ligesom de kan fastlægge de procedurer, der skal følges.

Et **harmoniseret og forenklet system** kunne reducere omkostningerne og de administrative byrder, især for multinationale virksomheder, som opererer i flere medlemsstater.

*Kommissionen vil undersøge forskellige muligheder for at **forenkle og harmonisere det nuværende anmeldelsessystem**, herunder for at udfærdige et **fælles EU-registreringsskema**.*

2.2.3. Præcisering af reglerne om gældende national ret og af medlemsstaternes ansvar

Kommissionen pegede allerede i første beretning om gennemførelsen af databeskyttelsesdirektivet i 2003[26] på, at bestemmelserne om gældende national ret[27], "i mange tilfælde er mangelfuld med det resultat, at den type lovkonflikter, som denne artikel søger at undgå, kan opstå". Situationen er ikke forbedret siden, og derfor står det ikke altid klart for de registeransvarlige og databeskyttelsesmyndighederne, hvilke myndigheder der er ansvarlige, og hvilken national ret der finder anvendelse, når flere medlemsstater er involveret. Det er særlig tilfældet, når de registeransvarlige er underkastet forskellige krav fra forskellige medlemsstaters side, når en multinational virksomhed er etableret i mere end en medlemsstat, eller når den registeransvarlige ikke er etableret i EU, men udbyder tjenester til personer, der er bosat i EU.

Globaliseringen og den teknologiske udvikling gør kun problemet endnu mere komplekst: De registeransvarlige opererer i stigende grad i flere medlemsstater og retskredse, hvor de udbyder tjenester og assistance hele døgnet. Internettet gør det langt lettere for registeransvarlige med sæde uden for Det Europæiske Økonomiske Samarbejdsområde[28] at udbyde tjenester på lang afstand og at behandle personoplysninger på internettet. Derfor er det ofte vanskeligt at afgøre, hvor personoplysninger og det it-udstyr, der anvendes på et givet tidspunkt (eksempelvis "cloud computing"-applikationer og tjenesteydelser), er fysisk placeret.

Kommissionen er af den opfattelse, at fysiske personer ikke bør berøves den beskyttelse, som de har krav på i henhold til EU's charter om grundlæggende rettigheder og EU's

---

25 Se artikel 18 i direktiv 95/46/EF.

26 Beretning fra kommissionen - Første beretning om gennemførelsen af databeskyttelsesdirektivet (95/46/EF) – KOM(2003) 265.

27 Se artikel 4 i direktiv 95/46/EF.

28 Det Europæiske Økonomiske Samarbejdsområde omfatter Norge, Liechtenstein og Island.

databeskyttelseslovgivning, blot fordi behandlingen af personoplysninger udføres af en registeransvarlig, der er etableret i et tredjeland.

Kommissionen vil undersøge, hvordan de **gældende bestemmelser om gældende national ret**, herunder de nuværende bestemmende kriterier, kan **revideres og præciseres** med henblik på at styrke retssikkerheden og tydeliggøre medlemsstaternes ansvar for at anvende databeskyttelsesreglerne, samt i sidste ende give de registrerede i EU-medlemsstater samme grad af beskyttelse, uanset hvor den registeransvarlige fysisk befinder sig.

2.2.4. Større ansvar til den registeransvarlige

Administrative forenklinger bør **ikke føre til, at de registeransvarliges ansvar for effektiv databeskyttelse samlet set mindskes**. Tværtimod finder Kommissionen, at de registeransvarliges forpligtelser bør præciseres i de relevante retsregler, herunder for så vidt angår interne kontrolmekanismer og samarbejde med databeskyttelsesmyndighederne. Desuden bør det sikres, at forpligtelserne også er gældende for registeransvarlige, som har tavshedspligt (f.eks. advokater), og i det stadigt stigende antal situationer, hvor den registeransvarlige overdrager databehandlingen til andre enheder (f.eks. registerførere).

Kommissionen vil derfor undersøge, hvordan det kan **sikres, at de registeransvarlige iværksætter effektive politikker og mekanismer, således at databeskyttelsesreglerne faktisk bliver overholdt.** I den forbindelse vil den tage bestik af debatten om en mulig indførelse at et "accountability-princip"[29]. Formålet med sådanne foranstaltninger er ikke at øge de administrative byrder for de registeransvarlige, men snarere at skabe sikkerhedsforanstaltninger og mekanismer, der mere effektivt sikrer overholdelsen af databeskyttelsesreglerne, samtidig med at visse administrative formaliteter (f.eks. anmeldelser) begrænses og forenkles (*se 2.2.2. ovenfor*).

Fremme af anvendelsen af teknologier til beskyttelse af privatlivets fred kan, som Kommissionen allerede gjorde opmærksom på i sin meddelelse om emnet i 2007, spille en vigtig rolle i så henseende, herunder i sikringen af datasikkerheden, og det samme kan princippet om "indbygget databeskyttelse"[30].

Med henblik på at øge de registeransvarliges ansvar vil Kommissionen undersøge muligheden for:

– at gøre det obligatorisk at udpege en **databeskyttelsesansvarlig** og harmonisere reglerne for de databeskyttelsesansvarliges opgaver og beføjelser[31], men samtidig overveje, hvor

29 Se særlig udtalelse 3/2010, som artikel 29-gruppen vedtog den 13. juli 2010.

30 Om anvendelse af teknologier til beskyttelse af privatlivets fred, se Kommissionens meddelelse til Europa-Parlamentet og Rådet om bedre databeskyttelse med teknologier til beskyttelse af privatlivet (KOM(2007) 228. Princippet om indbygget databeskyttelse indebærer, at hensynet til privatlivets fred og databeskyttelse indarbejdes i alle faser af en teknologis livscyklus, fra den første udformning til indførelse på markedet, brug og bortskaffelse. Princippet optræder blandt andet i Kommissionens meddelelse "En digital dagsorden for Europa" – KOM(2010) 245.

31 Den nuværende mulighed for, at en registeransvarlig kan udnævne en databeskyttelsesansvarlig, således at der på uafhængig vis sikres overholdelse af EU's og medlemsstaternes databeskyttelsesregler, og således at fysiske personer kan opnå hjælp, er allerede gennemført i flere medlemsstater (se f.eks. "Beauftragter für den Datenschutz" (tilsyn med databeskyttelse) i Tyskland og den tilsvarende "correspondant informatique et libertés" (CIL) i Frankrig).

bagatelgrænsen bør gå for at undgå unødige administrative byrder, navnlig for små virksomheder og mikrovirksomheder

– at lade retsreglerne omfatte en forpligtelse for de registeransvarlige til at foretage en **konsekvensanalyse, for så vidt angår databeskyttelse** i bestemte tilfælde, eksempelvis når følsomme oplysninger behandles, eller når arten af databehandling på anden måde indebærer særlige risici, herunder særlig når der anvendes specifikke teknologier, mekanismer eller procedurer, deriblandt profilering eller videoovervågning

– yderligere at fremme anvendelsen af teknologier til beskyttelse af privatlivets fred og mulighederne for at gennemføre begrebet "**indbygget databeskyttelse**" i praksis.

2.2.5. Større selvregulering og mulighed for EU-certificeringsordninger

Kommissionen er fortsat af den opfattelse, at registeransvarliges **selvregulering** kan **bidrage til bedre håndhævelse af databeskyttelsesreglerne**. De gældende bestemmelser om selvregulering i databeskyttelsesdirektivet, nemlig muligheden for udarbejdelse af adfærdskodekser[32], er hidtil sjældent blevet anvendt, og private interessenter finder dem ikke tilfredsstillende.

Desuden vil Kommissionen undersøge muligheden for at indføre EU-**certificeringsordninger (f.eks. "datasikkerhedsmærkninger")** for processer, teknologi, produkter og tjenesteydelser, der respekterer privatlivets fred[33]. De ville ikke blot vejlede den enkelte bruger af sådan teknologi og sådanne processer, produkter og tjenesteydelser, men kunne også være relevante i forhold til de registeransvarliges ansvar. Ved at vælge certificerede teknologier, produkter eller tjenesteydelser kunne den registeransvarlige bedre godtgøre, at han har opfyldt sine forpligtelser *(se 2.2.4. ovenfor)*. Det er naturligvis særdeles vigtigt at **sikre datasikkerhedsmærkningernes troværdighed** og undersøge, hvordan de kan passe sammen med juridiske forpligtelser og internationale tekniske standarder.

Kommissionen vil:

– undersøge, hvordan man kan **tilskynde yderlige til selvregulering**, herunder aktivt fremme adfærdskodekser

– undersøge, om det er muligt at oprette **EU-certificeringsordninger** for at beskytte privatlivets fred og datasikkerheden.

2.3. Revision af databeskyttelsesreglerne inden for politisamarbejdet og det retlige samarbejde i straffesager

Databeskyttelsesdirektivet finder anvendelse på al behandling af personoplysninger i medlemsstaterne både i den offentlige og den private sektor. Det finder dog ikke anvendelse på behandling af personoplysninger ved aktiviteter på områder, der ikke er omfattet af fællesskabsretten, såsom politisamarbejde og retligt samarbejde i straffesager[34].

[32] Se artikel 27 i direktiv 95/46/EF.

[33] Om dette aspekt henvises også til Se Kommissionens meddelelse om bedre databeskyttelse med teknologier til beskyttelse af privatlivet, jf. fodnote 29.

[34] Se artikel 3, stk. 2, første led, i direktiv 95/46/EF.

Lissabontraktaten har imidlertid afskaffet EU's tidligere "søjlestruktur" og indført et nyt og omfattende retsgrundlag for beskyttelse af personoplysninger på tværs af EU's politikker[35].

På denne baggrund og i lyset af EU's charter om grundlæggende rettigheder, har Kommissionen i sine meddelelser om Stockholmprogrammet og Stockholmhandlingsplanen[36] understreget behovet for at have en "omfattende beskyttelsesordning" og for at "styrke EU's holdning til beskyttelse af personoplysninger inden for rammerne af alle EU-politikker, herunder retshåndhævelse og kriminalitetsforebyggelse, og i vores internationale relationer".

EU's instrument til beskyttelse af personoplysninger inden for politisamarbejde og retligt samarbejde i straffesager er **rammeafgørelse 2008/977/RIA**[37]. Rammeafgørelsen er et vigtigt fremskridt på et område, hvor der er et stort behov for fælles standarder for databeskyttelse. Der er dog behov for yderligere tiltag på området.

Rammeafgørelsen finder kun anvendelse på grænseoverskridende udveksling af personoplysninger inden for EU og ikke på databehandling i de enkelte medlemsstater. I praksis er det dog vanskeligt at foretage en sådan skelnen, der risikerer at komplicere den faktiske gennemførelse og anvendelse af rammeafgørelsen[38].

Rammeafgørelsens fravigelse af formålsbegrænsningsprincippet er desuden for omfattende. Et andet problem er de manglende bestemmelser om, at der bør skelnes mellem forskellige kategorier af oplysninger ud fra, i hvor høj grad disse er korrekte og pålidelige, at oplysninger, der bygger på kendsgerninger bør skelnes fra oplysninger, der bygger på holdninger eller personlige vurderinger[39], og at der bør skelnes mellem de forskellige kategorier af registrerede (kriminelle, mistænkte, ofre, vidner osv.) med særlige garantier for oplysninger om personer, der ikke er mistænkte[40].

Hertil kommer, at **rammeafgørelsen ikke afløser de forskellige sektorspecifikke lovgivningsmæssige instrumenter inden for det politimæssige og strafferetlige samarbejde, som er vedtaget på EU-niveau**[41], særlig de instrumenter, der fastlægger Europols, Eurojusts, Schengeninformationssystemets og toldinformationssystemets[42] funktionsmåde, og som enten har særlige databeskyttelsesordninger, og/eller som normalt henviser til Europarådets databeskyttelsesinstrumenter. Med hensyn til aktiviteter inden for politisamarbejdet og det retlige samarbejde har alle medlemsstater bundet sig til at følge

---

35 Se artikel 16 i traktaten om Den Europæiske Unions funktionsmåde.

36 Se KOM(2009) 262 af 10.6.2009 og KOM(2010) 171 af 20.4.2010.

37 Rådets rammeafgørelse 2008/977/RIA af 27.11.2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i straffesager, EUT L 350 af 30.12.2008, s. 60. Rammeafgørelsen opererer udelukkende med en minimumsharmonisering af databeskyttelsesstandarderne.

38 Den nævnte skelnen findes ikke i de relevante europarådsinstrumenter såsom: Europarådets konvention om beskyttelse af individet i forbindelse med automatisk databehandling af personoplysninger (CETS nr. 108), Tillægsprotokollen vedrørende tilsynsmyndigheder og grænseoverskridende dataudveksling (ETS nr. 181) og Ministerkomitéens henstilling nr. R (87) 15 om politiets brug af personoplysninger, der blev vedtaget den 17. september 1987.

39 Jf. kravet i princip 3.2 i Ministerkomitéens henstilling nr. R (87) 15.

40 I modstrid med princip 2 i Ministerkomitéens henstilling nr. R (87) 15 og evalueringsrapporterne hertil.

41 Instrumenterne omtales i Kommissionens meddelelse "Oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed", KOM(2010) 385.

42 Der er oprettet fælles tilsynsmyndigheder ved de relevante instrumenter med henblik på at sikre kontrol med databeskyttelsen udover de generelle kontrolbeføjelser, som Den Europæiske Tilsynsførende for Databeskyttelse har over EU-institutioner, -organer, -kontorer og -agenturer i henhold til forordning (EF) nr. 45/2001.

Europarådets henstillinger nr. R (87) 15, som fastlægger principperne for Europarådskonvention nr. 108 for så vidt angår politisektoren. Der er dog ikke tale om et retligt bindende instrument.

Denne situation kan direkte påvirke fysiske personers muligheder for at udøve deres databeskyttelsesrettigheder på dette området (eksempelvis med hensyn til viden om, hvilke af deres personoplysninger der behandles og udveksles, af hvem og med hvilket formål, og om, hvordan de kan udøve deres rettigheder, såsom retten til at få adgang til deres oplysninger).

Målet om at skabe et omfattende og sammenhængende system inden for EU og i forhold til tredjelande gør det **nødvendigt at overveje en revision af de gældende databeskyttelsesregler inden for politisamarbejde og retligt samarbejde i straffesager**. Kommissionen vil gerne understrege, at det, at databeskyttelsesordningen skal være omfattende, ikke udelukker, at de generelle regler kan omfatte særlige databeskyttelsesregler for politisektoren og retsvæsenet, som tager hensyn til disse områders særlige karakter, jf. erklæring 21, der er knyttet som bilag til Lissabontraktaten. Det betyder bl.a., at det er nødvendigt at overveje, i hvilket omfang en fysisk persons udøvelse af sine databeskyttelsesrettigheder vil kunne skade forebyggelse, efterforskning, afsløring eller retsforfølgelse i straffesager eller fuldbyrdelse af strafferetlige sanktioner i konkrete sager.

Kommissionen vil navnlig:

– overveje at **udvide anvendelsen af de generelle databeskyttelsesregler til områderne politisamarbejde og retligt samarbejde i straffesager**, herunder databehandling i den enkelte medlemsstat, samtidig med, at der om nødvendigt foretages harmoniserede **begrænsninger** i nogle af de databeskyttelsesrettigheder, som fysiske personer har, eksempelvis vedrørende adgang til oplysninger eller gennemsigtighedsprincippet

– undersøge behovet for at indføje **specifikke og harmoniserede bestemmelser** i de nye generelle regler for databeskyttelse, f.eks. vedrørende databeskyttelse i forbindelse med behandling af **genetiske data** til strafferetlige formål eller skelnen mellem de forskellige kategorier af registrerede (vidner, mistænkte osv.) inden for politisamarbejde og retligt samarbejde i straffesager

– i 2011 iværksætte en **høring** af alle interessenter om, hvordan man bedst kan revidere de nuværende **kontrolordninger inden for politisamarbejde og retligt samarbejde i straffesager**. Målet er at sikre effektiv og konsekvent kontrol med databeskyttelse i alle EU-institutioner, -organer, -kontorer og –agenturer

– vurdere behovet for på længere sigt at **tilnærme** de **eksisterende forskellige sektorspecifikke EU-regler for politisamarbejde og retligt samarbejde i straffesager** til de nye generelle regler for databeskyttelse.

2.4. Databeskyttelsens globale dimension

2.4.1. Præcisering og forenkling af reglerne for internationale dataoverførsler

Et af midlerne til at muliggøre overførsel af personoplysninger uden for EU og EØS er den såkaldte "**vurdering af, om beskyttelsesniveauet er tilstrækkeligt**". Om et tredjeland giver databeskyttelse, som EU finder tilstrækkeligt, afgøres i dag af Kommissionen og medlemsstaterne.

Hvis Kommissionen finder, at databeskyttelsen er tilstrækkelig, kan de pågældende personoplysninger frit overføres fra de 27 EU-medlemsstater og de 3 EØS-medlemsstater til det pågældende tredjeland uden yderligere sikkerhedsforanstaltninger. I databeskyttelsesdirektivet er de præcise krav, der skal opfyldes, for at Kommissionen finder databeskyttelsen tilstrækkeligt, dog ikke formuleret tilstrækkeligt detaljeret. Hertil kommer, at rammeafgørelsen ikke opererer med, at Kommissionen skal træffe en sådan afgørelse.

I visse medlemsstater er det i første omgang den registeransvarlige, som vurderer, om databeskyttelsen er tilstrækkelig, og som selv overfører personoplysninger til et tredjeland, evt. under efterfølgende kontrol fra datakontrolmyndighedernes side. Denne situation kan føre til, at vurderingen af, hvorvidt tredjelandes eller internationale organisationers databeskyttelse er tilstrækkelig, vurderes forskelligt, og **dermed er der risiko for, at de registreredes beskyttelsesniveau i et tredjeland bedømmes forskelligt fra medlemsstat til medlemsstat**. De nuværende retlige instrumenter indeholder desuden ingen detaljerede og harmoniserede krav, der siger noget om, hvornår overførsler kan anses for at være i overensstemmelse med loven. Det indebærer, at praksis varierer fra medlemsstat til medlemsstat.

Derudover er Kommissionens gældende standardbestemmelser for overførsel af personoplysninger til registeransvarlige[43] og registerførere[44] i tredjelande, der ikke sikrer et passende beskyttelsesniveau, ikke beregnet på situationer uden for kontraktforhold og kan eksempelvis ikke anvendes på dataoverførsler mellem offentlige forvaltninger.

Desuden er der i de internationale aftaler, som EU eller EU's medlemsstater indgår, ofte krav om, at de skal indeholde databeskyttelsesprincipper og særlige bestemmelser. Det kan give forskellige tekster med inkonsekvente bestemmelser og rettigheder, hvilket kan føre til forskellige fortolkninger til skade for de registrerede. Derfor har Kommissionen meddelt, at den vil arbejde for at indføje en række kerneelementer vedrørende beskyttelse af personoplysninger i aftaler mellem EU og tredjelande med henblik på retshåndhævelse[45].

Der er udviklet andre midler som en form for selvregulering, f.eks. interne adfærdskodekser for virksomheder, de såkaldte "bindende virksomhedsregler"[46], som ligeledes kan være et nyttigt redskab til på lovlig vis at overføre personoplysninger mellem virksomheder inden for samme koncern. Interessenter har dog antydet, at denne mekanisme kan forbedres yderligere og gøres lettere at gennemføre.

---

43 Kommissionens beslutning af 15. juni 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF (EFT L 181 af 4.7.2001, s. 19), Kommissionens beslutning 2002/16/EF af 27. december 2001 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til direktiv 95/46/EF (EFT L 6 af 10.1.2002, s. 52), Kommissionens beslutning 2004/915/EF af 27. december 2004 om ændring af beslutning 2001/497/EF for at indføre en alternativ standardkontrakt om overførsel af personoplysninger til tredjelande (EUT L 385 af 29.12.2004, s. 74).

44 Kommissionens afgørelse af 5. februar 2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (EUT L 39 af 12.2.2010, s. 5).

45 Stockholmhandlingsplanen (jf. fodnote 36).

46 "Bindende virksomhedsregler" er adfærdskodekser, der bygger på databeskyttelsesstandarder, og som multinationale organisationer frivilligt udfærdiger og følger med henblik på at skabe passende sikkerhedsforanstaltninger for overførsler eller for kategorier af overførsler af personoplysninger mellem virksomheder, der indgår i samme koncern, og som er bundet af de pågældende virksomhedsregler. Se også: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

For at kunne løse de problemer, der er blevet afdækket, **er det generelt nødvendigt at forbedre de nuværende mekanismer til internationale overførsler af personoplysninger**, samtidig med at det skal sikres, at personoplysninger nyder passende beskyttelse, når de overføres og behandles uden for EU og EØS.

Kommissionen agter at undersøge:

– hvordan **de nuværende procedurer i forbindelse med internationale dataoverførsler kan forbedres og strømlines**, herunder i form af retligt bindende instrumenter og "bindende virksomhedsregler", så **EU's metode i forhold til tredjelande og internationale organisationer bliver mere ensartet og sammenhængende**.

– hvordan **Kommissionens procedure** til vurdering af, om databeskyttelsesniveauet i et tredjeland eller en international organisationer er tilstrækkeligt, **kan tydeliggøres**, herunder hvordan de **krav og kriterier**, der anvendes ved vurderingerne, kan udspecificeres

– hvordan **kerneelementer vedrørende EU's databeskyttelse**, der kan anvendes ved alle typer af internationale aftaler, kan defineres.

2.4.2. Fremme af universelle principper

Ligesom databehandlingen er globaliseret, bør der også udvikles universelle principper for beskyttelsen af fysiske personer med hensyn til behandling af personoplysninger.

Tredjelande har ofte brugt EU's retsregler for databeskyttelse som **benchmark ved regulering af databeskyttelse**. De har haft stor betydning og gennemslagskraft både i og uden for EU. Derfor er det vigtigt, at **Den Europæiske Union fortsat spiller en ledende rolle i udviklingen og fremme af internationale juridiske og tekniske standarder for beskyttelse af personoplysninger**, der bygger på relevante EU-databeskyttelsesinstrumenter og andre europæiske databeskyttelsesinstrumenter. Dette er særlig vigtigt i forbindelse med EU's udvidelsespolitik.

For så vidt angår de internationale tekniske standarder, der er udarbejdet af standardiseringsorganer, finder Kommissionen, at det er særdeles vigtig at skabe sammenhæng mellem de fremtidige retsregler og sådanne standarder, for at de registeransvarlige reelt kan gennemføre databeskyttelsesreglerne konsekvent.

Kommissionen vil:

– fortsat **fremme udviklingen af høje retlige og tekniske databeskyttelsesstandarder** i tredjelande og internationalt

– arbejde for **princippet om gensidighed i beskyttelsen i EU's internationale foranstaltninger**, herunder særlig for så vidt angår registrerede, hvis data overføres fra EU til tredjelande

– for at nå dette mål øge samarbejdet med tredjelande og internationale organisationer såsom OECD, Europarådet, De Forenede Nationer og regionale organisationer

– **nøje følge standardiseringsorganers** (f.eks. CEN og ISO) **udvikling af internationale tekniske standarder**, så det sikres, at de supplerer retsreglerne hensigtsmæssigt, og at de vigtigste databeskyttelseskrav rent faktisk gennemføres effektivt.

2.5. En stærkere institutionel ordning til bedre håndhævelse af databeskyttelsesreglerne

Gennemførelsen og håndhævelsen af databeskyttelsesprincipper og -regler er afgørende for at sikre overholdelse af fysiske personers rettigheder.

I den sammenhæng spiller **databeskyttelsesmyndighederne en særdeles vigtig rolle** i håndhævelsen af databeskyttelsesreglerne. De er uafhængige vogtere af de grundlæggende rettigheder og frihedsrettigheder med relation til beskyttelse af personoplysninger, og fysiske personer er afhængige af, at disse myndigheder sikrer, at deres personoplysninger beskyttes, og at databehandlingen foregår lovligt. Derfor finder Kommissionen, at deres rolle bør styrkes, ikke mindst i lyset af Domstolens seneste retspraksis vedrørende deres uafhængighed[47], og de bør have de nødvendige beføjelser og ressourcer, således at de på forsvarlig vis kan varetage deres opgaver både nationalt og i samarbejde med andre nationale databeskyttelsesmyndigheder.

Samtidig er Kommissionen af den opfattelse, at **databeskyttelsesmyndighederne bør intensivere deres indbyrdes samarbejde og koordinere deres arbejde bedre**, ikke mindst når de står over for problemer, som i deres natur har en grænseoverskridende dimension. Det er særlig tilfældet, når multinationale virksomheder har sæde i flere medlemsstater og opererer i hvert af disse lande, eller når der er krav om at koordinere kontrollen med Den Europæiske Tilsynsførende for Databeskyttelse[48].

I den henseende kan **artikel 29-gruppen**[49] spille en vigtig rolle. Ud over sin rådgivende funktion[50] har gruppen allerede til opgave at arbejde for, at EU's databeskyttelsesregler anvendes på samme måde i de enkelte medlemsstater. De fortsatte forskelle i databeskyttelsesmyndighedernes anvendelse og fortolkning af EU-reglerne viser, at det, på trods af at problemerne med databeskyttelse er de samme i hele EU, er nødvendigt at styrke artikel 29-gruppens koordinerende rolle i forhold til de nationale databeskyttelsesmyndigheder. Det kan sikre en mere ensartet anvendelse på nationalt niveau og dermed en ensartet databeskyttelse.

Kommissionen vil undersøge:

– hvordan **de nationale databeskyttelsesmyndigheders status og beføjelser kan styrkes, tydeliggøres og harmoniseres** i de nye retsregler, herunder hvordan begrebet "fuld uafhængighed" kan gennemføres fuldt ud[51]

– hvordan **samarbejdet og koordineringen mellem databeskyttelsesmyndighederne** kan forbedres

---

47 Se Domstolens dom af 9.3.2010, Kommissionen mod Tyskland, sag C-518/07.

48 Det er i øjeblikket tilfældet for store it-systemer, eksempelvis for SIS II, jf. artikel 46 i forordning (EF) nr. 1987/2006 (EUT L 318 af 28.12.2006, s. 4) og for VIS, jf. artikel 43 i forordning (EF) nr. 767/2008 (EUT L 218 af 13.8.2008, s. 60).

49 Artikel 29-gruppen er et rådgivende organ, der består af repræsentanter for medlemsstaternes databeskyttelsesmyndigheder, Den Europæiske Tilsynsførende for Databeskyttelse og Kommissionen (uden stemmeret). Kommissionen stiller sekretariatsfaciliteter til rådighed. Se også: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 Artikel 29-gruppen rådgiver Kommissionen om beskyttelsesniveauet i EU og i tredjelande og om foranstaltninger, der har at gøre med behandling af personoplysninger.

51 Se Domstolens dom af 9.3.2010, Kommissionen mod Tyskland, sag C-518/07.

– **hvordan** det kan sikres, at EU's databeskyttelsesregler anvendes mere konsekvent i hele det indre marked. Dette kan indebærer en **styrkelse af den rolle, som de nationale tilsynsførende for databeskyttelse spiller, en bedre koordinering af deres arbejde via artikel 29-gruppen (som bør blive et mere åbent organ), og/eller indførelse af en mekanisme, der under Europa-Kommissionens ledelse kan sikre konsekvens i det indre marked**.

3. KONKLUSION: VEJEN FREM

I lighed med teknologien ændrer den måde, som personoplysninger anvendes på og videregives i vores samfund, sig konstant. Udfordringen for lovgivere er at skabe langtidsholdbar lovgivning. Når reformprocessen er tilendebragt, bør EU's databeskyttelsesregler fortsat kunne sikre et højt beskyttelsesniveau og retssikkerhed for både fysiske personer, offentlig forvaltning og erhvervsliv på det internationale marked i flere generationer. Uanset hvor komplekse situationer, der opstår, eller hvor avanceret teknologi, der er tale om, skal der herske klarhed over de gældende regler og standarder, som de nationale myndigheder skal håndhæve, og som erhvervslivet og teknologiudviklere skal overholde. Også for fysiske personer skal det stå klart, hvilke rettigheder de har.

Kommissionens globale metode til at løse de problemer og nå de hovedmål, der er peget på i denne meddelelse, vil danne grundlag for yderligere drøftelser med de øvrige EU-institutioner og andre interessenter og skal senere munde ud i konkrete forslag og foranstaltninger af lovgivningsmæssig og ikke-lovgivningsmæssig art. Derfor modtager Kommissionen gerne feedback på de spørgsmål, der rejses i denne meddelelse.

På dette grundlag vil Kommissionen, efter en konsekvensanalyse og under hensyntagen til EU's charter om grundlæggende rettigheder, i **2011 foreslå lovgivning**, der har til formål at revidere retsreglerne om databeskyttelse, med det formål at styrke EU's holdning til beskyttelse af personoplysninger inden for rammerne af alle EU-politikker, herunder retshåndhævelse og kriminalitetsforebyggelse under hensyntagen til disse områders særlige karakter. Ikke-lovgivningsmæssige foranstaltninger, f.eks. tilskyndelse til selvregulering og muligheden for EU-datasikkerhedsmærkning, vil også blive undersøgt.

I anden omgang vil Kommissionen vurdere **behovet for at tilpasse andre retlige instrumenter** til den nye generelle regler for databeskyttelse. Det angår for det første forordning (EF) nr. 45/2001, hvis bestemmelser skal tilpasses de nye generelle retsregler. Konsekvenserne for andre sektorspecifikke instrumenter skal ligeledes undersøges nøje senere.

Kommissionen vil fortsat føre passende kontrol med, at EU-retten gennemføres korrekt på dette område, idet den **ikke vil tøve med at indlede traktatbrudssager**, når EU-reglerne for databeskyttelse ikke implementeres eller anvendes korrekt. Den igangværende revision af databeskyttelsesinstrumenterne fritager faktisk ikke medlemsstaterne fra forpligtelsen til at gennemføre og sikre den korrekte anvendelse af de eksisterende retlige instrumenter om beskyttelse af personoplysninger[52].

Et højt og ensartet databeskyttelsesniveau i EU er den bedste måde at støtte og fremme EU's databeskyttelsesstandarder på globalt.

[52] Det omfatter også Rådets rammeafgørelse 2008/977/RIA: Medlemsstaterne træffer de nødvendige foranstaltninger for at efterkomme denne rammeafgørelse inden den 27. november 2010.