EUROPA-KOMMISSIONEN

Bruxelles, den 25.1.2012
COM(2012) 9 final

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

Beskyttelse af privatlivets fred i en forbundet verden
En europæisk databeskyttelsesramme til det 21. århundrede

(EØS-relevant tekst)

[…]

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

Beskyttelse af privatlivets fred i en forbundet verden
En europæisk databeskyttelsesramme til det 21. århundrede

(EØS-relevant tekst)

1. AKTUELLE UDFORDRINGER MED HENSYN TIL DATABESKYTTELSE

Den teknologiske udvikling og globaliseringen foregår i så højt et tempo, at det har revolutioneret måden, hvorpå vi indsamler, får adgang til, udnytter og videregiver en stedse stigende mængde personoplysninger. Nye måder at udveksle oplysninger gennem sociale netværk og fjernopbevare store mængde data på er blevet en del af hverdagen for mange af Europas 250 mio. internetbrugere. Samtidig er personoplysningerne blevet et aktiv for mange virksomheder. Indsamling, organisering og analysering af oplysninger om potentielle kunder er ofte en stor del af deres økonomiske aktiviteter[1].

I dette nye digitale miljø **har fysiske personer ret til effektiv kontrol over deres egne personoplysninger.** Databeskyttelse er en grundlæggende rettighed i Europa, der er forankret i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF), og denne rettighed skal således beskyttes.

Manglende tillid får forbrugerne til at være tilbageholdende med at købe varer på internettet og benytte nye tjenester. Derfor er et højt databeskyttelsesniveau afgørende for, om befolkningen får mere tillid til onlinetjenesterne, og om den digitale økonomi kan udnytte sit potentiale og dermed skabe incitament til **økonomisk vækst og bedre konkurrenceevne i EU's erhvervsliv.**

Der er brug for moderne, sammenhængende regler for hele EU, så dataene kan flyde frit mellem medlemsstaterne. Virksomhederne har brug for klare og ensartede regler, der giver retssikkerhed og minimerer den administrative byrde. Det er meget vigtigt, hvis det indre marked skal fungere godt og kunne **skabe økonomisk vækst, nye job og innovation**[2]. En modernisering af EU's databeskyttelsesregler, så de får større vægt i det indre marked, sikrer et højt databeskyttelsesniveau for fysiske personer og fremmer retssikkerheden og den retlige klarhed og sammenhæng, spiller derfor en

---

[1] Markedet for analyse af meget store datasæt vokser med 40 % om året på verdensplan. http://www.mckinsey.com/mgi/publications/big_data/.

[2] Se også Det Europæiske Råds konklusioner af 23. oktober 2011, hvori Rådet understreger "den centrale rolle", som det indre marked spiller, "når det gælder om at skabe vækst og beskæftigelse", foruden behovet for at fuldføre det digitale indre marked inden 2015.

central rolle i Europa-Kommissionens Stockholmprogram[3], i den digitale dagorden for Europa[4] og mere generelt i EU's vækststrategi (Europa 2020)[5].

EU's direktiv fra 1995[6], som er den centrale retsakt vedrørende beskyttelse af personoplysninger i Europa, var en milepæl i databeskyttelsens historie. Målene med direktivet, som var at sikre et velfungerende indre marked og en effektiv beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder, gælder stadig. Det blev imidlertid vedtaget for 17 år siden, da internettet trådte sine barnesko. I det nye, udfordrende digitale miljø, vi oplever i dag, giver de bestående regler hverken den nødvendige grad af harmonisering eller den fornødne gennemslagskraft til at sikre fysiske personers ret til databeskyttelse. Derfor foreslår Europa-Kommissionen en grundlæggende reform af EU's databeskyttelsesramme.

Desuden har Lissabontraktaten i medfør af artikel 16 i TEUF skabt et nyt retsgrundlag for en moderniseret og global metode til databeskyttelse og fri udveksling af personoplysninger, som også omfatter politimæssigt og retligt samarbejde i straffesager[7]. Denne metode er afspejlet i Europa-Kommissionens meddelelser om Stockholmprogrammet og handlingsplanen dertil[8], hvori den understreger behovet for, at Unionen "bør have en komplet ordning for beskyttelse af personoplysninger på samtlige EU's kompetenceområder" og "skal sikre, at den grundlæggende ret til databeskyttelse overholdes konsekvent".

For at forberede reformen af EU's databeskyttelsesramme på en gennemsigtig måde har Kommissionen siden 2009 afholdt offentlige høringer om databeskyttelse[9] og ført en tæt dialog med interessenterne[10]. Den 4. november 2010 offentliggjorde Kommissionen en meddelelse om en global metode til beskyttelse af personoplysninger i Den Europæiske Union[11], som indeholdt hovedtemaerne for reformen. Mellem september og december 2011 deltog Kommissionen i en udvidet dialog med Europas nationale databeskyttelsesmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse for at undersøge mulighederne for en mere ensartet anvendelse af EU's databeskyttelsesregler i alle EU-medlemsstater[12].

---

3 COM(2010) 171 final.

4 COM(2010) 245 final.

5 COM(2010) 2020 final.

6 Direktiv 95/46/EF 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.

7 Der skal fastlægges specifikke regler for medlemsstaternes databehandling inden for EU's fælles udenrigs- og sikkerhedspolitiske område i en afgørelse fra Rådet baseret på artikel 39 i TEU.

8 COM(2009) 262 og COM(2010) 171.

9 Der er iværksat to offentlige høringer om databeskyttelsesreformen: en fra juli til december 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) og en fra november 2010 til januar 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 Der blev afholdt målrettede høringer i 2010 blandt medlemsstaternes myndigheder og private interessenter. I november 2010 tilrettelagde EU's kommissær for retlige anliggender Viviane Reding en rundbordsdrøftelse om reformen af databeskyttelsesrammen. Der blev også arrangeret målrettede workshopper og seminarer om specifikke spørgsmål (f.eks. anmeldelse af brud på datasikkerheden) i løbet af 2011.

11 COM(2010) 609.

12 Se brevet fra EU's kommissær for retlige anliggender Viviane Reding af 19. september 2011 til medlemmerne af "Artikel 29-gruppen" på: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

Disse drøftelser gjorde det klart, at både borgere og virksomheder ønskede, at Europa-Kommissionen skulle gennemføre en altomfattende reform af EU's databeskyttelsesregler. Efter at have foretaget en konsekvensanalyse[13] af de forskellige løsningsmodeller foreslår Europa-Kommissionen nu **en stærk og konsekvent retlig ramme på tværs af EU's politikker, der styrker fysiske personers rettigheder, databeskyttelsens vægt i det indre marked og bekæmpelsen af bureaukrati for erhvervslivet**[14]**.** Kommissionen foreslår, at den nye ramme skal bestå af:

– en **forordning** (der erstatter direktiv 95/46/EF) om en generel EU-ramme for databeskyttelse[15]

– og et **direktiv** (der erstatter rammeafgørelse 2008/977/RIA[16]) om beskyttelse af personoplysninger, der behandles med henblik på **forebyggelse, opdagelse, efterforskning eller retsforfølgning af straffelovsovertrædelser og tilknyttede retslige aktiviteter**.

Denne meddelelse indeholder de primære elementer i reformen af EU's databeskyttelsesramme.

2. FYSISKE PERSONER SKAL KUNNE KONTROLLERE DERES PERSONOPLYSNINGER

Siden vedtagelsen af direktiv 95/46/EF – EU's primære retsakt på databeskyttelsesområdet i dag – er der ikke sket en tilstrækkelig harmonisering mellem medlemsstaterne af de muligheder, som fysiske personer har for at udøve deres ret til databeskyttelse. De nationale myndigheders beføjelser på databeskyttelsesområdet er heller ikke blevet harmoniseret i en grad, der har kunnet sikre, at reglerne anvendes ensartet og effektivt. Det betyder, at det reelt er sværere at udøve sine rettigheder i nogle medlemsstater end i andre, særligt online.

Alene mængden af data, der indsamles hver dag, vanskeliggør databeskyttelsen, foruden at brugerne ofte ikke er helt klar over, at der indsamles personoplysninger om dem. Selv om mange europæere mener, at videregivelse af personoplysninger i stigende grad er en del af det moderne liv[17], er der stadig 72 % af de europæiske internetbrugere, der er bekymrede over, at de bliver bedt om at udlevere for mange

---

13 Se konsekvensanalysen (SEK(2012) 72).

14 Dette vil siden hen indebære indførelse af ændringer med henblik på at afstemme de specifikke og sektorale instrumenter efter hinanden, bl.a. forordning (EF) nr. 45/2001 (EFT L 8 af 12.1.2001, s. 1).

15 Forordningen indeholder også et begrænset antal tekniske tilpasninger til e-databeskyttelsesdirektivet (direktiv 2002/58/EF, senest ændret ved direktiv 2009/136/EF – EUT L 337 af 18.12.2009, s. 11), således at der nu er taget hensyn til, at direktiv 95/46/EF er ændret til en forordning. De omfattende retlige følger af den nye forordning og det nye direktiv for e-databeskyttelsesdirektivet vil senere blive gennemgået af Kommissionen, og her vil den tage hensyn til resultatet af forhandlingerne om de forslag, der nu er til drøftelse i Europa-Parlamentet og Rådet.

16 Rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager (EUT L 350 af 30.12.2008, s. 60). En rapport om medlemsstaternes gennemførelse af rammeafgørelsen (COM(2012) 12) vedtages som led i databeskyttelsesreformpakken.

17 Se Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union, juni 2011, s. 23.

personoplysninger over nettet[18]. De synes ikke, de selv bestemmer over deres personoplysninger. De får ikke ordentlig besked om, hvad der sker med deres personoplysninger, hvem de videregives til, og med hvilket formål. Ofte ved de ikke, hvordan de skal udøve deres rettigheder online.

"Retten til at blive glemt"

En europæisk studerende, som er medlem af et socialt netværk på internettet, beslutter at anmode om adgang til alle de personoplysninger, som netværket har om ham. Derved finder han ud af, at netværket indsamler mange flere oplysninger, end han var klar over, og at nogle af personoplysningerne, som han troede, han havde slettet, stadig opbevares.

Reformen af EU's databeskyttelsesregler vil sikre, at det ikke længere forekommer, ved at der indføres:

– et udtrykkeligt krav om, at onlinetjenester i form af sociale netværk (og alle andre, der indsamler data) skal minimere den mængde personoplysninger om brugerne, de indsamler og behandler

– et krav om, at standardindstillingerne skal sikre, at personoplysninger ikke offentliggøres

– en udtrykkelig pligt, der pålægges de registeransvarlige, til at slette en fysisk persons personoplysninger, hvis vedkommende udtrykkeligt anmoder om sletning, og når der ikke er andre legitime grunde til at opbevare oplysningerne.

I eksemplet ville udbyderen af det sociale netværk således være forpligtet til straks at slette den studerendes personoplysninger fuldstændig.

Som det fremhæves i den digitale dagsorden for Europa, er bekymringen for privatlivets fred blandt de hyppigste grunde til, at folk undlader at købe varer og tjenester online. Med informations- og kommunikationsteknologisektorens bidrag til den samlede produktivitetsstigning i Europa – 20 % fra ikt-sektoren og 30 % fra ikt-investeringerne[19] – er tilliden til disse tjenester helt afgørende for stimuleringen af den europæiske økonomiske vækst og europæisk erhvervslivs konkurrenceevne.

Anmeldelse af brud på datasikkerheden

Der har været et hackerangreb på en spilletjeneste, som henvender sig til brugere i EU. Bruddet på datasikkerheden gik ud over databaser med personoplysninger (bl.a. navne, adresser og muligvis kreditkortoplysninger) på mange millioner brugere over hele verden. Virksomheden ventede en uge med at underrette de berørte brugere.

Reformen af EU's databeskyttelsesregler vil sikre, at det ikke længere forekommer. Ifølge de nye regler pålægges virksomhederne:

– at skærpe deres sikkerhedsforanstaltninger med henblik på at forebygge og undgå brud

– uden unødig forsinkelse at underrette både den nationale databeskyttelsesmyndighed – inden for 24 timer efter at bruddet er opdaget, hvis det er muligt – og de berørte fysiske personer .

Målet med Kommissionens foreslåede nye retsakt er at styrke rettighederne, give befolkningen effektive og operationelle midler til at sikre sig, at de er fuldt informerede om, hvad der sker med deres personoplysninger, og sætte dem i stand til at udøve deres rettigheder mere effektivt.

[18] Ibidem, s. 54.

[19] Se den digitale dagsorden for Europa, s. 4.

For at styrke fysiske personers ret til databeskyttelse foreslår Kommissionen nye regler, som skal:

øge fysiske personers kontrol over deres personoplysninger ved at

- sikre, at et **samtykke**, når der er krav om et sådant, **gives udtrykkeligt, hvilket vil sige, at det afgives i form af en erklæring eller ved en klar, bekræftende handling fra den berørte persons side**, og at det gives frivilligt

- udstyre internetbrugerne med en reel **ret til at blive glemt** i onlinemiljøet, hvilket vil sige retten til at få deres personoplysninger slettet, hvis de trækker deres samtykke tilbage, og hvis der ikke er andre legitime grunde til at opbevare personoplysningerne

- garantere **let adgang til ens egne personoplysninger** og en **ret til dataportabilitet**, hvilket vil sige ret til at få en kopi af de opbevarede personoplysninger fra den registeransvarlige og frihed til uhindret at flytte dem fra én tjenesteudbyder til en anden

- skærpe **retten til information**, så fysiske personer fuldt ud forstår, hvordan deres personoplysninger behandles, især når databehandlingen angår **børn**.

forbedre fysiske personers midler til at udøve deres rettigheder ved at

- styrke de nationale **databeskyttelsesmyndigheders uafhængighed og beføjelser**, så de har de fornødne instrumenter til effektiv håndtering af klager og de rette beføjelser til at udføre effektive undersøgelser, træffe bindende afgørelser og pålægge effektive og afskrækkende sanktioner

- styrke de **administrative instrumenter og retsmidler** til brug i tilfælde af **overtrædelse** af databeskyttelsesrettighederne. Især skal kvalificerede foreninger kunne indbringe en sag for domstolen på vegne af fysiske personer.

skærpe datasikkerheden ved at

- tilskynde til brug af **teknologier, der kan forbedre beskyttelsen af privatlivets fred** (teknologier, der beskytter private oplysninger ved at minimere opbevaringen af personoplysninger), **standardindstillinger, der begunstiger privatlivets fred**, og **certificeringsordninger vedrørende privatlivets fred**

- pålægge registeransvarlige **en generel pligt**[20] til **uden unødig forsinkelse** (hvilket normalt er inden for 24 timer) at **underrette** både databeskyttelses-myndighederne og de berørte fysiske personer **om brud på datasikkerheden**.

[20] Denne forpligtelse findes i øjeblikket kun i telekommunikationssektoren i medfør af e-databeskyttelsesdirektivet.

øge registerføreres ansvarlighed, især ved at

- kræve, at de registeransvarlige udpeger en **databeskyttelsesansvarlig** i virksomheder med over 250 ansatte og i virksomheder, som er involveret i behandlingen, som på grund af dens art, omfang eller formål indebærer særlige risici, hvad angår enkeltpersoners rettigheder og friheder ("risikobehæftet behandling")

- indføre **princippet om "Privacy by Design"** (privatlivsbeskyttelse indbygget i it-arkitekturen) for at sikre, at der tages hensyn til databeskyttelsen allerede i planlægningsfasen til nye procedurer og systemer

- pålægge organisationer, der udfører risikobehæftet databehandling, en pligt til at foretage **konsekvensanalyser vedrørende databeskyttelse**.

3. DATABESKYTTELSESREGLER, DER EGNER SIG TIL DET DIGITALE INDRE MARKED

Trods målet med det gældende direktiv om at sikre et ensartet databeskyttelsesniveau i hele EU er der stadig store forskelle på reglerne medlemsstaterne imellem. Derfor kan de registeransvarlige være nødt til at henholde sig til 27 forskellige nationale sæt af love og krav. Resultatet er et **fragmenteret lovgivningsmiljø**, som har skabt **manglende retssikkerhed** og en uensartet beskyttelse af fysiske personer. Resultatet er **unødige omkostninger og administrative byrder** for erhvervslivet, og det fratager virksomheder i det indre marked incitamentet til at ekspandere på tværs af grænserne.

De enkelte medlemsstaters nationale databeskyttelsesmyndigheder har meget forskellige ressourcer og beføjelser[21]. I visse tilfælde er de ikke i stand til at udøve deres håndhævelsesopgaver tilfredsstillende. Samarbejdet mellem disse myndigheder på EU-plan – via den eksisterende rådgivende gruppe (den såkaldte Artikel 29-gruppe)[22] – er ikke altid nok til at sikre en ensartet håndhævelse og skal også forbedres.

Ensartet håndhævelse af databeskyttelsesreglerne i hele Europa

Et multinationalt selskab med flere afdelinger i EU indførte et onlinekortlægningssystem i hele Europa, hvori der indsamles billeder af alle private og offentlige bygninger, og hvor også folk på gaden kan være blevet fotograferet. I én medlemsstat ansås det for ulovligt at indsamle ikke-slørede billeder af personer, der ikke var klar over, at de blev fotograferet, mens det i en anden medlemsstat ikke udgjorde et brud på databeskyttelsesreglerne. Derfor kunne de nationale databeskyttelsesmyndigheder ikke håndtere denne situation på en ensartet måde.

Reformen af EU's databeskyttelsesregler vil sikre, at denne situation ikke forekommer i fremtiden, idet:

---

21 Der kan læses mere om dette aspekt i den konsekvensanalyse, der ledsager lovforslagene, SEC(2012) 72.

22 Artikel 29-gruppen blev nedsat i 1996 (ved artikel 29 i direktiv 95/46/EF) med status af rådgivende organ og består af repræsentanter for de nationale databeskyttelsesmyndigheder, Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) og Kommissionen. Se yderligere oplysninger om gruppens aktiviteter på http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

– der vil blive fastlagt databeskyttelseskrav og -foranstaltninger i en EU-forordning, der finder direkte anvendelse i hele Unionen

– det kun er databeskyttelsesmyndigheden i det land, hvor selskabet har sit hovedkontor, der skal afgøre, om selskabet handler lovligt

– en øjeblikkelig og effektiv koordinering mellem de nationale databeskyttelsesmyndigheder – idet tjenesten er rettet mod fysiske personer i flere medlemsstater – skal sikre, at de nye EU-regler om databeskyttelse anvendes og håndhæves ensartet i alle medlemsstater.

De nationale myndigheder skal styrkes og deres samarbejde udbygges med henblik på at garantere en ensartet håndhævelse og i sidste ende fuldstændig ens anvendelse af reglerne i hele EU.

En stærk, klar og ensartet retlig ramme på EU-plan vil bidrage til, at det digitale indre markeds potentiale kan udnyttes, og der kan skabes økonomisk vækst, innovation og beskæftigelse. En forordning vil fjerne fragmenteringen af retssystemerne i de 27 medlemsstater og fjerne hindringerne for markedsadgang, hvilket er særlig vigtigt for mikrovirksomheder og små og mellemstore virksomheder.

De nye regler vil også give EU's erhvervsliv en fordel i den globale konkurrence. Med den reformerede lovgivning vil de kunne forsikre deres kunder om, at værdifulde personoplysninger vil blive behandlet med den fornødne omhu og grundighed. At der er tillid til en ensartet EU-lovgivning på området vil være et vigtigt aktiv for tjenesteudbyderne og et incitament for investorer, der ønsker optimale vilkår, når tjenesterne skal placeres geografisk.

For at lægge større vægt på **databeskyttelse som led i det indre marked** foreslår Kommissionen at:

- fastlægge databeskyttelsesregler på EU-plan gennem en **forordning, der finder direkte anvendelse i alle medlemsstater**[23], og som dermed kan sætte en stopper for kumulativ og samtidig anvendelse af forskellige nationale databeskyttelseslove. Det vil udløse en **nettobesparelse for virksomhederne på ca. 2,3 mia. EUR om året alene i kraft af en mindre administrativ byrde**

- **forenkle lovgivningsmiljøet ved at skære drastisk ned på bureaukratiet** og fjerne **formaliteter** som den generelle anmeldelsespligt (med deraf følgende nettobesparelser på 130 mio. EUR om året alene i kraft af en mindre administrativ byrde). I lyset af betydningen heraf for europæisk økonomis konkurrenceevne lægges der særlig vægt på de specifikke behov, mikrovirksomheder og små og mellemstore virksomheder har

- **styrke de nationale databeskyttelsesmyndigheders uafhængighed og beføjelser yderligere** for at sætte dem i stand til at udføre effektive undersøgelser, træffe bindende afgørelser og iværksætte effektive og afskrækkende sanktioner og pålægge medlemsstaterne at forsyne dem med de **nødvendige ressourcer** til opgaven

[23] Der foreslås et direktiv om fastlæggelse af reglerne for politimæssigt og retligt samarbejde i straffesager (se afsnit 4 nedenfor), som kan give medlemsstaterne mere fleksibilitet på netop dette område.

- **oprette et databeskyttelsessystem af typen one-stop-shop i EU:** De registeransvarlige i EU skal kun henvende sig til **en enkelt databeskyttelses-myndighed**, nemlig databeskyttelsesmyndigheden i den medlemsstat, hvor selskabets hovedkontor har adresse

- skabe betingelser for et **hurtigt og effektivt samarbejde mellem databeskyttelsesmyndighederne,** bl.a. ved at pålægge dem pligt til at foretage undersøgelser og tilsyn på anmodning fra andre databeskyttelsesmyndigheder og gensidigt anerkende hinandens afgørelser

- **indføre en sammenhængsmekanisme på EU-plan for at sikre, at databeskyttelsesmyndigheder** i beslutninger med en bredere europæisk indvirkning tager hensyn til andre berørte databeskyttelsesmyndigheder, og at beslutningerne fuldt ud er i overensstemmelse med EU-retten

- opgradere Artikel 29-gruppen til et **uafhængigt europæisk databeskyttelses-råd** for at forbedre gruppens bidrag til den ensartede anvendelse af databeskyttelsesloven og danne et stærkt fundament for samarbejdet mellem databeskyttelsesmyndighederne, herunder Den Europæiske Tilsynsførende for Databeskyttelse, og øge synergieffekten og effektiviteten ved at sørge for, at Den Europæiske Tilsynsførende for Databeskyttelse varetager sekretariatsfunktionen for Det Europæiske Databeskyttelsesråd.

Den nye EU-forordning sikrer en robust beskyttelse af den grundlæggende ret til databeskyttelse i hele Den Europæiske Union og styrker det indre markeds funktion. Da retten til beskyttelse af personoplysninger som det blev understreget af EU-Domstolen[24] samtidig ikke udgør en absolut ret, men skal ses i sammenhæng med sin funktion i samfundet[25] og afvejes mod andre grundlæggende rettigheder, jf. proportionalitetsprincippet[26], kommer forordningen til at indeholde udtrykkelige bestemmelser, som sikrer overholdelsen af andre grundlæggende rettigheder såsom ytringsfrihed og informationsfrihed og retten til forsvar samt tavshedspligt (f.eks. for advokater) uden at anfægte kirkernes status i henhold til medlemsstaternes love.

4. ANVENDELSE AF DATA I DET POLITIMÆSSIGE OG RETLIGE SAMARBEJDE I STRAFFESAGER

Lissabontraktatens ikrafttræden og især indførelsen af et nyt retsgrundlag (artikel 16 i TEUF) giver mulighed for at fastlægge en omfattende databeskyttelsesramme til sikring af et højt databeskyttelsesniveau for fysiske personer, samtidig med at den specifikke karakter af politimæssigt og retligt samarbejde i straffesager respekteres.

---

24 EU-Domstolens dom af 9.11.2011, forenede sager C-92/09 og C-93/09, Volker und Markus Schecke og Eifert [2010], endnu ikke trykt i Samlingen.

25 I henhold til artikel 52, stk. 1, i chartret, kan der indføres begrænsninger i udøvelsen af retten til databeskyttelse, forudsat at de er fastlagt i lovgivningen, respekterer disse rettigheders og friheders væsentligste indhold og under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

26 EU-Domstolens dom af 6.11.2003, C-101/01, Lindqvist, Sml. 2003 I, s. 12971, præmis 82-90; dom af 16.12.2008, C-73/07, Satamedia, Sml. 2008 I, s. 9831, præmis 50-62.

Det gør det bl.a. muligt at lade den ændrede EU-ramme for databeskyttelse omfatte behandling af personoplysninger både på tværs af grænserne og nationalt. Det vil mindske forskellene i lovgivningen i medlemsstaterne, hvilket skulle blive til gavn for beskyttelsen af personoplysninger generelt. Det kan også føre til en smidigere informationsudveksling mellem medlemsstaternes politimyndigheder og retsmyndigheder og dermed forbedre samarbejdet i bekæmpelsen af alvorlig kriminalitet i Europa. Politimyndigheders og retsmyndigheders behandling af data i straffesager er i øjeblikket primært omfattet af rammeafgørelse 2008/977/RIA, som ligger før Lissabontraktatens ikrafttræden. Kommissionen har ingen beføjelser til at håndhæve reglerne heri, da det er en rammeafgørelse, og denne situation har bidraget til en uensartet gennemførelse. Desuden er rammeafgørelsens anvendelsesområde begrænset til grænseoverskridende databehandling[27]. Det betyder, at behandlingen af personoplysninger, der ikke er blevet udvekslet, i øjeblikket ikke er omfattet af EU-reglerne om sådan databehandling og om beskyttelse af den grundlæggende ret til databeskyttelse. Det skaber i visse tilfælde også vanskeligheder i praksis for politiet og andre myndigheder, for hvem det måske ikke er indlysende, om databehandlingen er rent national eller går på tværs af grænserne, eller som måske ikke kan forudse, at "nationale" data kan blive genstand for en senere udveksling på tværs af grænserne[28].

EU's nye, reformerede databeskyttelsesramme har derfor til formål at sikre et ensartet, højt databeskyttelsesniveau for at **styrke den gensidige tillid mellem politi- og retsmyndigheder i de forskellige medlemsstater og dermed bidrage yderligere til den frie udveksling af data og et effektivt samarbejde mellem politi og retsvæsen**.

For at sikre et højere beskyttelsesniveau for personoplysninger på området politimæssigt og retligt samarbejde i straffesager og lette udvekslingen af personoplysninger mellem medlemsstaternes politimyndigheder og retsmyndigheder foreslår Kommissionen som led i databeskyttelsesreformpakken at udstede et direktiv, hvori:

- det fastlægges, **at de generelle databeskyttelsesprincipper finder anvendelse** på politimæssigt og retligt samarbejde i straffesager, idet disse områders specifikke karakter respekteres[29]

- der fastlægges **harmoniserede minimumskriterier og -betingelser for eventuelle begrænsninger** af de almindelige regler. Dette vedrører især fysiske personers ret til at blive informeret, når politimyndigheder og retsmyndigheder behandler eller har adgang til deres personoplysninger. Disse begrænsninger er nødvendige af hensyn til en effektiv forebyggelse, efterforskning, opdagelse eller retsforfølgning af straffelovsovertrædelser

---

27 Nærmere betegnet finder rammeafgørelsen anvendelse på personoplysninger, der "videregives eller er videregivet eller stilles til rådighed eller er stillet til rådighed mellem medlemsstater" eller udveksles mellem medlemsstaterne og EU's institutioner eller organer (se artikel 1, stk. 2).

28 Dette blev bekræftet af visse medlemsstater i besvarelsen af det spørgeskema, som Kommissionen har udsendt med henblik på rapporten om gennemførelsen af rammeafgørelsen (COM(2012) 12).

29 Se erklæring 21 om beskyttelse af personoplysninger inden for politimæssigt og retligt samarbejde i straffesager knyttet som bilag til slutakten fra den regeringskonference, der vedtog Lissabontraktaten.

- indføre **specifikke regler, som dækker retshåndhævelsesaktiviteternes særlige karakter, herunder en sondring mellem forskellige kategorier af registrerede**, hvis rettigheder kan variere (f.eks. vidner og mistænkte).

5. DATABESKYTTELSE I EN GLOBALISERET VERDEN

Fysiske personers rettigheder skal fortsat garanteres, når personoplysninger overføres fra EU til tredjelande, og når det er fysiske personer i medlemsstaterne, der er målgruppen, og deres personoplysninger anvendes eller analyseres af tjeneste-udbydere i tredjelande. Det betyder, at EU's databeskyttelsesstandarder skal finde anvendelse uanset selskabets eller dets databehandlingsenheds geografiske beliggenhed.

I nutidens globaliserede verden overføres personoplysninger på tværs af et stigende antal virtuelle og geografiske grænser og opbevares på servere i mange lande. Flere og flere virksomheder tilbyder cloud computing-tjenester, hvorved kunderne får fjernadgang til servere med henblik på at opbevare data "i skyen". Disse faktorer kræver en forbedring af de aktuelle mekanismer til overførsel af data til tredjelande, bl.a. afgørelser om tilstrækkeligheden af beskyttelsesniveauet – dvs. afgørelser om, at databeskyttelsesstandarden er "tilstrækkelig" i tredjelande – og fornødne garantier såsom standardkontraktbestemmelser eller bindende virksomhedsregler[30], således at der kan sikres et højt databeskyttelsesniveau i international databehandling, og datastrømmen på tværs af grænserne lettes.

Bindende virksomhedsregler

En selskabskoncern har jævnligt brug for at overføre personoplysninger fra sine selskaber i EU til andre af koncernens selskaber i tredjelande. Koncernen vil gerne indføre et sæt bindende virksomhedsregler for at overholde EU-lovgivningen og begrænse de administrative krav til hver enkelt overførsel. I praksis sikrer bindende virksomhedsregler, at ét sæt regler gælder i hele koncernen og ikke for hver enkelt intern kontrakt.

På baggrund af den aktuelle praksis, der er aftalt i Artikel 29-gruppen, kræves det for at få en anerkendelse af, at et selskabs bindende virksomhedsregler giver en tilstrækkelig beskyttelse, at tre databeskyttelsesmyndigheder (en ledende og to assisterende) foretager en grundig gennemgang af reglerne, men disse kan også kommenteres af flere andre databeskyttelsesmyndigheder. Desuden kræver mange medlemsstaters love yderligere nationale tilladelser til de overførsler, der er omfattet af bindende virksomhedsregler, og det gør vedtagelsesprocessen meget omstændelig, dyr, langstrakt og kompleks..

Efter databeskyttelsesreformen:

– vil denne proces blive enklere og mere strømlinet

– vil de bindende virksomhedsregler kun blive valideret af én databeskyttelsesmyndighed, og der vil være mekanismer til sikring af hurtig inddragelse af andre relevante databeskyttelsesmyndigheder

30 Bindende virksomhedsregler er praksiskodekser, der er baseret på europæiske databeskyttelses-standarder, godkendt af mindst én databeskyttelsesmyndighed og udarbejdet på frivillig basis af organisationer, som følger kodekserne for at sikre en tilstrækkelig beskyttelse af de typer overførsel af personoplysninger, som foregår mellem selskaber, der indgår i samme selskabskoncern og er bundet af disse regler. De er ikke udtrykkeligt omfattet af direktiv 95/46/EF, men har udviklet sig i praksis mellem databeskyttelsesmyndighederne med støtte fra Artikel 29-gruppen.

– vil en bindende virksomhedsregel efter en enkelt databeskyttelsesmyndigheds godkendelse være gyldig i hele EU uden yderligere tilladelser på nationalt plan.

For at kunne **tage globaliseringens udfordringer op** skal vi indføre fleksible redskaber og mekanismer – især til virksomheder, der opererer i hele verden – og samtidig garantere en beskyttelse af personoplysninger, der er uden smuthuller. Kommissionen foreslår følgende foranstaltninger:

- **klare regler,** der definerer, **hvornår EU-retten gælder for register-ansvarlige, der er etableret i tredjelande,** især ved at det præciseres, at der, hver gang fysiske personer tilbydes varer og tjenesteydelser i EU, elle hver gang deres adfærd overvåges, skal **EU-reglerne anvendes**

- enhver **afgørelse om tilstrækkeligheden af beskyttelsesniveauet** vil blive truffet af Europa-Kommissionen på grundlag af udtrykkelige og klare kriterier, bl.a. inden for politimæssigt og retligt samarbejde i straffesager

- en styrkelse og forenkling af **reglerne om international overførsel** til lande, der ikke er omfattet af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, vil lette de lovlige datastrømme til tredjelande, især i kraft af en mere strømlinet og omfattende udnyttelse af redskaber som **bindende virksomhedsregler**, så de kan bruges til at dække **registerførere** og **koncerninterne** overførsler, hvilket vil give en bedre afspejling af det stigende antal selskaber, der benytter databehandling, især cloud computing

- indledning af **dialog** og i fornødent omfang af **forhandlinger** med tredjelande – især EU's strategiske partnere og lande, de er omfattet af den europæiske naboskabspolitik – og relevante internationale organisationer (såsom Europarådet, OECD og FN) for at **fremme høje og interoperable databeskyttelsesstandarder** på verdensplan.

6. KONKLUSION

Formålet med EU's databeskyttelsesreform er at opbygge **en moderne, stærk, sammenhængende og omfattende databeskyttelsesramme for Den Europæiske Union**. Fysiske personer skal kunne udøve deres grundlæggende ret til databeskyttelse. Andre rettigheder som ytringsfrihed, informationsfrihed, børns rettigheder, retten til at drive virksomhed, retten til en retfærdig rettergang og tavshedspligt (f.eks. for advokater) samt kirkernes status i henhold til medlemsstaternes love vil blive respekteret.

Reformen vil først og fremmest gavne fysiske personer ved at styrke deres databeskyttelsesrettigheder og øge deres tillid til det digitale miljø. Reformen vil desuden forenkle lovgivningsmiljøet betydeligt for erhvervslivet og den offentlige sektor. Dette forventes at stimulere udviklingen af den digitale økonomi i og uden for EU's indre marked i overensstemmelse med målsætningerne i Europa 2020-strategien og den digitale dagsorden for Europa. Endelig vil reformen forstærke den indbyrdes tillid mellem de retshåndhævende myndigheder for derved at lette dataudvekslingen mellem dem og forbedre samarbejdet om bekæmpelse af alvorlig kriminalitet og samtidig sikre et højt databeskyttelsesniveau for fysiske personer.

Europa-Kommissionen vil arbejde tæt sammen med Europa-Parlamentet og Rådet om at sikre en aftale om EU's nye databeskyttelsesramme inden udgangen af 2012. I løbet af denne vedtagelsesproces og i tiden efter, især i forbindelse med gennemførelsen af de nye retlige instrumenter, vil Kommissionen til stadighed opretholde en **tæt og åben dialog med alle interessenter**, bl.a. repræsentanter fra den private og den offentlige sektor. Der er her tale om repræsentanter fra politi og retsvæsen, tilsynsmyndigheder for elektronisk kommunikation, civilsamfunds-organisationer, databeskyttelsesmyndigheder og den akademiske verden samt EU's specialiserede agenturer som f.eks. Eurojust, Europol, Agenturet for Grundlæggende Rettigheder og Det Europæiske Agentur for Net- og Informationssikkerhed.

I en tid med konstant informationsteknologisk udvikling og foranderlige sociale adfærdsmønstre er en sådan dialog yderst vigtig og nødvendig, idet inputtene fra dialogen skal udnyttes til at opnå et højt databeskyttelsesniveau for fysiske personer, skabe vækst og konkurrenceevne i EU's erhvervsliv, fremme operationel effektivitet i den offentlige sektor (herunder politi og retsvæsen) og sikre en minimal administrativ byrde.