Østre Landsret
Præsidenten

Den 22 MAJ 2012
J.nr. 40A-ØL-28-12
Init: cr

Justitsministeriet
Civil- og Politiafdelingen
EU-formandssekretariatet
Slotsholmsgade 10
1216 København K

Justitsministeriet har ved brev af 11. maj 2012 (sagsnr. 2012-3756-0005) anmodet om eventuelle bemærkninger til Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

I den anledning skal jeg meddele, at forslaget ikke giver landsretten anledning til at fremkomme med bemærkninger.

Med venlig hilsen

Bent Carlsen

Ellen Bueck Porsbo

Bredgade 59, 1260 København K. Tlf. 33 97 02 00 (Fax 33 14 58 22) Hjemmeside: www.oestrelandsret.dk

Vestre Landsret
Præsidenten

Justitsministeriet
Civil- og Politiafdelingen
Slotsholmsgade 10
1216 København K

J.nr. 40A-VL-26-12
Den 12/06-2012

Justitsministeriet har ved brev af 11. maj 2012 anmodet om eventuelle bemærkninger til et forslag fra Europa-Kommissionen til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

I den anledning skal jeg meddele, at forslaget ikke giver landsretten anledning til at fremkomme med bemærkninger.

Dette svar sendes alene elektronisk og til jm@jm.dk

Der henvises til j.nr. 2012-3756-0005.

Med venlig hilsen

Bjarne Christensen

RIGSPOLITIET

POLITI

Justitsministeriet
Slotsholmsgade 10
1216 København K

e-mail: jm@jm.dk

J.nr.: 2012-005-754

3. juli 2012

RIGSPOLITIET
CENTER FOR ALMEN JURA
POLITITORVET 14
1780 KØBENHAVN V

Telefon: 3314 8888
Telefax: 4515 0017

Web: www.politi.dk

Ved brev af 11. maj 2012 har Justitsministeriet anmodet Rigspolitiet om eventuelle bemærkninger til Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

Rigspolitiet kan tilslutte sig de generelle betragtninger om bl.a. forslagets betydning for den offentlige sektor, der er anført i Justitsministeriets grund- og nærhedsnotat af 8. maj 2012.

Rigspolitiet kan herudover ikke umiddelbart pege på forhold, der særligt vil gøre sig gældende for politiets virksomhed.

Der henvises til Justitsministeriets sags.nr.: 2012-3756-0005.

Med venlig hilsen

Birgit Kleis
afdelingschef

RIGSADVOKATEN

Justitsministeriet
EU-formandsskabssekretariatet
Slotsholmsgade 10
1216 København K

DATO 10. juli 2012

JOURNAL NR.
RA-2012-1419-0074
BEDES ANFØRT VED SVARSKRIVELSER
SAGSBEHANDLER: ERK

RIGSADVOKATEN

FREDERIKSHOLMS KANAL 16
1220 KØBENHAVN K

TELEFON 33 12 72 00
FAX 33 43 67 10

Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) (sagsnr. 2012-3756-0005)

Justitsministeriet har ved e-mail af 11. maj 2012 anmodet om Rigsadvokatens eventuelle bemærkninger til Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

Jeg skal indledningsvis bemærke, at jeg finder det positivt, at der ved revisionen af databeskyttelsesreglerne i EU er valgt en løsning, hvor behandling mv. af personoplysninger inden for politiets og anklagemyndighedens område ikke – som udgangspunkt – reguleres af det generelle forordningsforslag, men at reguleringen i stedet foretages i forslag til direktiv om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger, der tillige er fremsat.

Det er således min opfattelse, at de særlige forhold omkring efterforskning og strafforfølgning af forbrydelser, der gør sig gældende på det politimæssige og strafferetlige område, bedst vil kunne varetages ved en særskilt regulering af området, således som

det også i dag er tilfældet, jf. hertil Rådets Rammeafgørelse af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejdet og retligt samarbejde i kriminalsager (databeskyttelsesrammeafgørelsen), og som det er forudsat i Lissabontraktatens 21. erklæring om beskyttelse af personoplysninger inden for retligt samarbejde i straffesager og politisamarbejde.

For så vidt angår formuleringen af den generelle undtagelse af det politimæssige og strafferetlige område fra forslaget til forordnings anvendelsesområde, jf. forslagets artikel 2, stk. 2, litra e) og præambelbetragtning nr. 16, skal jeg bemærke, at det fremgår heraf, at forordningen ikke finder anvendelse på behandling af personoplysninger, "som foretages af kompetente myndigheder med henblik på forebyggelse, efterforskning, opdagelse eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner".

Denne formulering er identisk med den formulering, der tidligere er anvendt i artikel 1, stk. 2, i databeskyttelsesrammeafgørelsen i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, der dog som udgangspunkt alene finder anvendelse på begrænsede grænseoverskridende aktiviteter af politimæssig eller strafferetlig karakter.

I artikel 3, stk. 2, i Europa-Parlamentets og Rådets direktiv af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesdirektivet), er det politimæssige og strafferetlige område generelt undtaget, idet databeskyttelsesdirektivet ikke finder anvendelse på "statens aktiviteter på det strafferetlige område".

Efter min opfattelse forekommer det herefter uklart, om den formulering, der er anvendt i forslaget til forordning, indebærer, at dele af behandlingen af personoplysninger indenfor det politimæssige og strafferetlige område vil være omfattet af forordningen. Det forekommer efter min opfattelse endvidere uklart, hvilken konkret afgrænsning, der skal foretages af forordningens anvendelsesområde overfor direktivforslagets.

Forslaget til forordning indeholder således bestemmelser, der synes at forudsætte, at forordningen kan finde anvendelse på behandling af personoplysninger inden for det politimæssige og strafferetlige område, jf. hertil f.eks. forslagets artikel 9 om behandling af personoplysninger om straffedomme, artikel 20 om profilering, artikel 21 om muligheden for at begrænse rækkevidden af visse rettigheder med henblik på "forebyggelse, efterforskning, opdagelse og retsforfølgning i straffesager", samt præambelbetragtning 87 sammenholdt med forslagets kapitel V om videregivelse af oplysninger inden for en koncern.

Jeg finder på den baggrund, at forordningens anvendelsesområde i forbindelse med de videre forhandlinger i EU bør nærmere afklares, således at det sikres, at det politimæssige og strafferetlige område fuldt ud undtages forordningen, således at reguleringen af området herefter alene sker i det kommende direktiv vedrørende om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger.

Med venlig hilsen

Alessandra Giraldi

Fra: Lisbeth Feldvoss [LFK@procesbevillingsnaevnet.dk]
Sendt: 25. maj 2012 16:27
Til: Justitsministeriet
Emne: Høringssvar - j.nr. 2012-3756-0005

Justitsministeriet ved Johan K. Legarth har ved brev af 11. maj 2012 anmodet Procesbevillingsnævnet om eventuelle bemærkninger til Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

I den anledning kan det oplyses, at Procesbevillingsnævnet ikke har bemærkninger hertil.

Med venlig hilsen

Lisbeth Feldvoss
Chefkonsulent

dommerfuldmægtigforeningen

Justitsministeriet
Civil- og Politiafdelingen
EU-formandsskabssekretariatet
Slotsholmsgade 10
1216 København K

København, den 24. juni 2012

Vedr. Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse), Deres sagsnr. 2012-3756-0005

Justitsministeriet har ved e-mail af 11. maj 2012 anmodet om Dommerfuldmægtigforeningens eventuelle bemærkninger til forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

Foreningen skal i den anledning meddele, at foreningen ikke har bemærkninger til forslaget.

Dette høringssvar sendes elektronisk til: jm@jm.dk med angivelse af sagsnr. 2012-3756-0005.

På foreningens vegne,

Stine Nielsen
Høringsansvarlig
Dommerfuldmægtigforeningen

DATATILSYNET

Justitsministeriet
Slotsholmsgade 10
1216 København K

Sendt til jm@jm.dk og cws@jm.dk

11. juli 2012

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2012-111-0013
2011-09-0074
Sagsbehandler
Lasse May
Direkte 3319 3214

Vedrørende forslag til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og den fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

1. Indledning

Den 11. maj 2012 har Justitsministeriet sendt Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og den fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) i høring hos bl.a. Datatilsynet. Med høringen fulgte endvidere Justitsministeriets grund- og nærhedsnotat om forslaget.

I det følgende gives i afsnit 2 Datatilsynets generelle bemærkninger vedrørende forordningen, mens afsnit 3 indeholder mere specifikke kommentarer til forslaget, og afsnit 4 omhandler forholdet til gældende lovgivning.

Herudover skal tilsynet henvise til sin udtalelse af 12. marts 2012 til Justitsministeriet om den foreløbige vurdering af de økonomiske konsekvenser for Datatilsynet af reformpakken om databeskyttelse.

Tilsynet henviser endvidere til Artikel 29-gruppens udtalelse af 23. marts 2012 om reformpakken, som er tilgængelig her: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

2. Generelle bemærkninger

I lyset af den teknologiske udvikling og globaliseringen er der efter Datatilsynets opfattelse god grund til at overveje reguleringen af databeskyttelsesområdet, således at borgerne sikres et højt beskyttelsesniveau samtidig med, at fordelene ved nye digitale løsninger og services kan høstes.

Datatilsynet hilser det således også velkomment, at forslaget til forordning indeholder en række elementer, som tilsigter at styrke borgernes retsstilling og retssikkerhed. For virksomheder, myndigheder og organisationer er der endvidere krav om at tage større ansvar for databeskyttelse ved i praksis at implementere databeskyttelsesfremmende initiativer samt udvise ansvarlighed ved behandling af personoplysninger. For at sikre efterlevelse af de foreslåede

regler lægges der op til styrkede beføjelser og sanktionsmuligheder for tilsynsmyndighederne.

Samtidig tilsigtes en smidiggørelse og en øget harmonisering af reglerne inden for EU til gavn for institutioner og virksomheder med aktiviteter på tværs af EU's grænser.

Valget af forordning som det retlige instrument tilsigter en høj grad af harmonisering. Tilsynet vurderer imidlertid, at det kan vise sig meget vanskeligt at sikre en ensartet databeskyttelsesregulering af mange forskellige sektorer i 27 EU-lande ved en generel forordning, der som det foreliggende forslag indeholder mange retlige standarder.

Som nævnt vil forslaget på flere områder medføre en styrkelse af borgernes rettigheder mv. Der er imidlertid også visse punkter, hvor forslaget vil træde i stedet for danske regler med et højere beskyttelsesniveau, og den foreslåede regulering – som den foreligger nu – derfor må siges at medføre en dårligere retsstilling for borgerne.

Endelig må det påpeges, at i forhold til såvel danske myndigheder og virksomheder som tilsynet vurderes forordningen samlet set at ville medføre en betydelig forøgelse af administrative byrder og ressourcebehov, jf. også nedenfor under pkt. 3.

I det følgende gives Datatilsynets mere specifikke kommentarer til en række af bestemmelserne i forslaget, idet det samtidig bemærkes, at yderligere analyse og afklaring synes påkrævet for at fastlægge den præcise rækkevidde af de foreslåede bestemmelser, jf. som også anført i Justitsministeriets grund- og nærhedsnotat, side 25 f.

3. Bemærkninger til bestemmelser i forordningsforslaget

3.1. Anvendelsesområdet

Forordningen inkluderer dataansvarlige, der ikke er etableret i Danmark eller EU, når de behandler oplysninger om personer bosiddende i EU, f.eks. i forbindelse med udbud af varer eller tjenester til sådanne registrerede i Unionen.

I Artikel 29-gruppens udtalelse er det bl.a. foreslået, at det tydeliggøres, at udbud af varer eller tjenester også omfatter gratis tjenester, hvor den registrerede i realiteten betaler for tjenesten ved at afgive sine personoplysninger.

Det er endvidere påpeget i Artikel 29-gruppens udtalelse (s. 18f), at anvendelsen af princippet om "one-stop shop" (artikel 51, stk. 2) bør overvejes i forhold til situationer omfattet af det udvidede anvendelsesområde.

Datatilsynet skal endvidere anbefale, at det indgår i de videre overvejelser om udvidelse af anvendelsesområdet, hvordan tilsynsmyndigheder i praksis kan håndhæve forordningen over for virksomheder uden for EU.

3.2. Definitioner

3.2.1. Registerbegrebet og forholdet til juridiske personer

Hos danske myndigheder og virksomheder findes sagsmapper og sagsakter, som er struktureret efter bestemte kriterier, men som falder uden for regulering i den gældende persondatalov. Dette skyldes tilkendegivelserne i forarbejderne til persondataloven, hvorefter manuelle akter, som indgår i den dataansvarliges konkrete sagsbehandling, mapper med sagsakter eller samlinger af sådanne mapper, ikke er omfattet af registerbegrebet.

Som eksempler kan nævnes papirbaserede personale- og kundemapper, der kan indeholde dokumenter mv. produceret over en længere årrække – dvs. fra før man foretog elektronisk databehandling.

Efter forslaget er det ikke længere overladt til medlemslandene at præcisere registerbegrebet, således som det er tilfældet med det gældende databeskyttelsesdirektiv, jf. direktivets betragtning 27.

Af betragtning 13 i det foreliggende forslag fremgår, at beskyttelsen af fysiske personer bør være teknologineutral og ikke afhænge af den anvendte teknik. Endvidere anføres, at "[B]eskyttelsen af fysiske personer bør gælde for både automatisk og manuel behandling af personoplysninger, hvis oplysningerne er indeholdt eller påtænkes indeholdt i et register. Sagsmapper eller samlinger af sagsmapper eller deres forsider, som ikke er struktureret efter bestemte kriterier, hører ikke under denne forordnings anvendelsesområde."

Spørgsmålet om afgrænsning af anvendelsesområdet i forhold til manuelle (papirbaserede) sagsakter og samlinger af sagsakter under den nuværende regulering har i praksis været rejst over for Datatilsynet i en del sager. I lyset af, at der nu foreslås en regulering i en forordning, finder Datatilsynet det helt centralt, at spørgsmålet om eventuel anvendelse af forordningens regler på strukturerede manuelle sagsmapper – eksempelvis personale- og kundemapper samt patientjournaler – afklares som led i forhandlingerne på EU-niveau.

Selv om mange virksomheder og myndigheder i dag hovedsageligt benytter elektronisk databehandling, findes der fortsat en stor mængde manuelle sagsmapper på arkiv hos myndighederne, og dette gør sig formentlig også gældende hos virksomhederne. I forhold til den gældende regulering i den danske persondatalov vil anvendelse af forslagets bestemmelser på sådanne manuelle sagsmapper bl.a. indebære, at der er indføres en indsigtsret i manuelle (papirbaserede) sager hos private virksomheder, som ikke findes i dag.

Hvis de strukturerede manuelle sagsmapper fuldt ud omfattes af reguleringen i såvel den offentlige som den private sektor, vil dette medføre et øget ressourceforbrug hos alle parter: myndigheder, virksomheder og Datatilsynet.

Datatilsynet finder det noget uklart, om forordningen tænkes anvendt på juridiske personer i videre omfang end det gældende direktiv. Rækkevidden af

betragtning 12 bør således afklares. Endvidere må den danske oversættelse af betragtningen efter tilsynets vurdering være forkert.

3.2.2. Genetiske og biometriske data
I forslaget introduceres definitioner af henholdsvis genetiske og biometriske data.

Datatilsynet finder, at begge definitioner bør analyseres nærmere, og beskrivelsen præciseres, hvis de skal indgå i forordningen. De forekommer meget omfattende/brede og har samtidig et betydeligt indbyrdes overlap, hvilket får betydning i forhold til behandlingsbetingelserne, jf. artiklerne 6 og 9. Biometriske data som eksempelvis fingeraftryk er hidtil blevet anset som almindelige, ikke-følsomme oplysninger, men vil efter tilsynets vurdering tillige være omfattet af den foreslåede definition på genetiske data og dermed skulle behandles som en følsom oplysning efter den foreslåede artikel 9.

3.2.3. Helbredsoplysninger
Den foreslåede definition af helbredsoplysninger er meget omfattende – navnlig når den sammenholdes med betragtning 26. Datatilsynet finder umiddelbart, at der ikke er grundlag for at udvide begrebet som foreslået.

3.2.4. Hovedvirksomhed
Der henvises til udtalelsen fra Artikel 29-gruppen, s. 10, om behovet for at præcisere definitionen.

3.2.5. Andre forhold
I forhold til de foreslåede definitioner i artikel 4, litra 15 (virksomhed), 16 (koncern) og 18 (barn) bør det efter Datatilsynets opfattelse overvejes, hvorvidt det er hensigtsmæssigt i forordningen at medtage definitioner af forhold, som må formodes at være defineret i andre generelle regelsæt.

Datatilsynet finder det uhensigtsmæssigt, at "controller" og "processor" i den danske udgave er oversat til "registeransvarlig" og registerfører". Disse begreber signalerer, at der alene er tale om en regulering af registre.

3.3. Interesseafvejning i offentlig sektor
I artikel 6, stk. 1, litra f), om den såkaldte interesseafvejningsregel indgår i sidste punktum en undtagelse fra reglen, således at den ikke gælder for den behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Hvis offentlige myndigheder ikke har mulighed for at anvende interesseafvejningsreglen som behandlingshjemmel, rejser det efter Datatilsynets opfattelse en række problemstillinger i forhold til gældende dansk praksis.

Offentlige myndigheder anvender i en række situationer interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7, som behandlings- og videregiveleshjemmel. Af eksempler kan nævnes: offentliggørelse af medarbejderoplysninger på internettet, offentliggørelse af afgørelser og postlister samt kontrol-

foranstaltninger i forhold til ansatte. Reglen har endvidere betydning i tilfælde, hvor spørgsmål om behandling af personoplysninger opstår som følge af bestemmelser i kollektive aftaler og overenskomster.

3.5. Betingelser for samtykke
Datatilsynet finder, at rækkevidden af artikel 7, stk. 4, sammenholdt med betragtning 34 bør afklares, da betragtning 34 oplister konkrete eksempler på, at samtykke ikke kan betragtes som gyldigt behandlingsgrundlag. Tilsynet gør opmærksom på, at gældende praksis efter persondataloven ikke er forenelig hermed.

3.6. Behandling af et barns personoplysninger
I den foreslåede artikel 8 indføres en aldersgrænse på 13 år i forhold til børns mulighed for på egen hånd at samtykke til direkte tilbud om informationssamsfundstjenester.

Datatilsynet er enig i, at internettet og andre former for digitale services kan give anledning til særlige problemstillinger i forhold til børn og unge mennesker. Det bør imidlertid overvejes og afklares, hvilken konsekvens en særregel som den foreslåede vil have for andre områder, hvor der opstår spørgsmål om børns retsstilling i forhold til behandling af personoplysninger, jf. herved også forslaget om at indsætte en generel definition af "barn". Datatilsynet har i praksis behandlet spørgsmål om eksempelvis børns selvstændige ret til indsigt og meddelelse efter reglerne om oplysningspligt.

3.7. Private virksomheders behandling af oplysninger om strafbare forhold
Datatilsynet finder, at konsekvenserne af artikel 9, stk. 2, litra j), bør afklares i relation til privates behandling af oplysninger om strafbare forhold. Herunder bør det overvejes, om bestemmelsen giver virksomhederne mulighed for at foretage behandling af disse oplysninger i samme omfang som i dag.

3.8. Behandling, der ikke muliggør identifikation
Datatilsynet finder den foreslåede præcisering i artikel 10 meget nyttig.

3.9. Elektronisk meddelelse af indsigt
I forhold til de foreslåede regler i artikel 12, stk. 2, og artikel 15, stk. 2, om, at elektronisk anmodning om indsigt skal besvares elektronisk, skal Datatilsynet pege på behovet for datasikkerhed ved besvarelse af indsigtsanmodninger. Herunder bl.a. sikring af, at oplysningerne ikke udleveres eller fremsendes til uvedkommende.

3.10. Ret til at blive glemt og ret til sletning
Det er Datatilsynets vurdering, at artikel 17 bør underkastes en nøje analyse som også påpeget i Artikel 29-gruppens udtalelse

Datatilsynet skal i den forbindelse også opfordre til, at rækkevidden af artikel 17, stk. 8, overvejes. Efter gældende regler, herunder arkivlovgivningen, forudsættes der opbevaret dokumentation, herunder personoplysninger, for sags-

behandlingen i forbindelse med en borgers anmodning om at blive glemt. Spørgsmålet er, om den foreslåede artikel 17, stk. 8, lægger op til, at sådan dokumentation ikke må opbevares.

3.11. Dataportabilitet

De foreslåede regler om dataportabilitet i forslagets artikel 18 giver en bredt formuleret ret til den registrerede til at få kopi af oplysninger, der er genstand for behandling, udleveret fra den dataansvarlige.

I Datatilsynets praksis er borgeren i en række tilfælde selv anset for dataansvarlig for de oplysninger, som han eller hun vælger at lade behandle i en tjeneste. Det kan f.eks. være dokumenter, som en borger overfører til sine elektroniske mapper i e-boks, eller billeder mv., som borgeren har valgt at placere i et online album eller i en cloud-løsning. Her vil borgerens ret til dataportabilitet efter tilsynets umiddelbare vurdering ikke følge af de foreslående regler.

Området for reglerne synes derimod at være alt muligt andet og synes umiddelbart at have et betydeligt overlap med retten til indsigt.

Datatilsynet går umiddelbart ud fra, at den dataansvarlige virksomhed eller myndighed i en række tilfælde fortsat vil have hjemmel til at behandle de personoplysninger, som den registrerede efter artikel 18, stk. 1 og 2, har fået kopi af. I givet fald bør dette tydeliggøres, og forholdet til "retten til at blive glemt" bør overvejes.

3.12. Øget ansvar til de dataansvarlige

I forslagets afsnit 2 findes – startende med artikel 22 – en række bestemmelser, som må antages at medvirke til en forbedret databeskyttelse, hvilket Datatilsynet bifalder.

3.13. Datasikkerhed

Efter den danske persondatalov har Justitsministeriet adgang til at fastsætte nærmere regler om de fornødne sikkerhedsforanstaltninger i bekendtgørelsesform. Dette er sket for den offentlige sektor i sikkerhedsbekendtgørelsen[1], der bl.a. indeholder en bestemmelse i § 4, hvorefter Datatilsynet har adgang til at komme med henstillinger over for den dataansvarlige myndighed vedrørende de trufne sikkerhedsforanstaltninger.

Efter forslaget har Kommissionen efter artikel 30, stk. 3, kompetence til at vedtage delegerede retsakter og efter artikel 30, stk. 4, adgang til om nødvendigt at vedtage gennemførelsesretsakter.

Datatilsynet skal opfordre til, at man fra dansk side overvejer hensigtsmæssigheden af, at kompetencen med hensyn til disse forhold tillægges Kommissionen. Det bør i den forbindelse sikres, at tilsynet ikke afskæres fra at stille konkrete krav til datasikkerheden via henstillinger eller lignende.

---

[1] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

3.14. Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

Efter artikel 31, stk. 1, i forslaget anmelder den dataansvarlige ved brud på persondatasikkerheden uden unødig forsinkelse og om muligt senest 24 timer – efter at denne er blevet bekendt med det – bruddet på persondatasikkerheden til tilsynsmyndigheden. Anmeldelsen til tilsynsmyndigheden ledsages af en begrundelse, hvis den ikke er indgivet inden for 24 timer.

Efter Datatilsynets opfattelse er det væsentligste ikke at få anmeldt et sikkerhedsbrud til tilsynet, men at den dataansvarlige tager behørigt affære og gør det nødvendige for at afbøde konsekvenserne af sikkerhedsbruddet. De skridt, der umiddelbart kan være påkrævede, kan være at påse, at data bliver slettet eller evt. afhentet/returneret fra uberettigede modtagere, at data slettes fra internet, herunder fra søgemaskiner, samt eventuelt – afhængigt af den konkrete situation – at sørge for en hurtig underretning af berørte personer. Dertil kommer de langsigtede skridt med henblik på at sikre, at situationen ikke gentager sig.

Ved at gøre underretning til tilsynsmyndigheden til det primære opstår der efter Datatilsynets opfattelse tvivl om, hvorvidt ansvaret for at tage hånd om situationen overlades til tilsynsmyndigheden, således at ingen umiddelbar reaktion fra tilsynsmyndigheden kan opfattes som om, at den dataansvarlige ikke behøver at foretage sig yderligere.

Datatilsynet finder således, at reglerne for den dataansvarliges håndtering af sikkerhedsbrud har fået en meget uheldig udformning i det foreliggende forslag.

Hertil kommer, at når *alle* brud på persondatasikkerheden – også små og relativt ubetydelige – skal anmeldes til Datatilsynet, vil det kræve et stort ressourceforbrug hos tilsynet at håndtere og i et vist omfang sagsbehandle disse anmeldelser. Der henvises herved tillige til tilsynets udtalelse af 12. marts 2012 om den foreløbige vurdering af de økonomiske konsekvenser for Datatilsynet af reformpakken om databeskyttelse. Som anført heri indebærer forslaget behov for ressourcer til et stående beredskab – formentlig i døgndrift.

Datatilsynet skal opfordre til, at det helt klart kommer til at fremgå, at det er den dataansvarlige, som har ansvaret for håndteringen af et sikkerhedsbrud, at håndtering, herunder meddelelse til evt. berørte registrerede, er det primære, og at en anmeldelsesordning i forhold til tilsynsmyndigheden kun omfatter de mere alvorlige sikkerhedsbrud og ikke berører den dataansvarliges ansvar til at agere i situationen.

Der henvises i den forbindelse til udtalelse nr. 1/2009 fra Artikel 29-gruppen, vedtaget 10. februar 2009, om forslagene om ændring af direktiv 2002/58/EF om databeskyttelse og elektronisk kommunikation (e-databeskyttelsesdirektivet), afsnit 2. Herudover indeholder Artikel 29-gruppens udtalelse, s. 16, bemærkninger om problemstillinger i forbindelse hermed.

Datatilsynet skal endvidere opfordre til, at forholdet til princippet om at undgå selvinkriminering afklares.

3.15. Konsekvensanalyse vedrørende databeskyttelse og forudgående godkendelse

Bestemmelserne i artikel 33 og 34 indfører en ny model for forudgående vurdering af behandlinger, der kan indebære nærmere beskrevne specifikke risici.

Datatilsynet ser som udgangspunkt positivt på den foreslåede model, hvor der skal gennemføres en konsekvensanalyse vedrørende databeskyttelse, når der er tale om nærmere beskrevne former for behandling, som kan indebære risici.

Tilsynet lægger imidlertid vægt på, at der ikke indføres en godkendelsesordning, hvor Datatilsynet skal have alle konsekvensanalyserne forelagt.

Datatilsynet skal derfor foreslå, at man fra dansk side arbejder for at få artikel 34, stk. 6, ændret, således at det klart fremgår, at de udformede konsekvensanalyser kun skal indgives til tilsynet, når tilsynet anmoder om dette, eller når analysen viser, at behandlingen indebærer store konkrete risici – i sidstnævnte tilfælde udløser dette høring efter artikel 34, stk. 2, litra a.

3.16. Databeskyttelsesansvarlige

I forordningens artikel 35 lægges der op til, at alle offentlige myndigheder, virksomheder med flere ansatte end 250 samt virksomheder, der har overvågning af registrerede som kerneaktivitet, skal udpege databeskyttelsesansvarlige. Disse personer skal medvirke til virksomhedens eller den offentlige myndigheds overholdelse af forordningen.

Datatilsynet bekendt er erfaringerne med ordninger med databeskyttelsesansvarlige positive i såvel Tyskland som Sverige og Norge. Tilsynet ser derfor positivt på den foreslåede ordning.

3.17. Datatilsynet

3.17.1. Forslaget til forordning indeholder adskillige bestemmelser, der berører tilsynets opgavevaretagelse, medfører nye opgaver og forpligtelser, og vil nødvendiggøre ændringer i tilsynets organisering mv. I udtalelsen af 12. marts 2012 til Justitsministeriet om den foreløbige vurdering af de økonomiske konsekvenser har Datatilsynet omtalt en række af de elementer, som påvirker tilsynets opgavevaretagelse. I det følgende fremhæves enkelte elementer – uden at der herved er tale om en udtømmende gennemgang af de bestemmelser, der forventes at medføre ændringer for tilsynet.

I forhold til tilsynsopgaver, som er beskrevet bl.a. i artikel 52, har Artikel 29-gruppen bl.a. påpeget, at det bør fremgå udtrykkeligt, at tilsynene har mulighed for at udføre inspektioner.

Herudover er det bl.a. fremhævet, at tilsynene bør være i stand til at være selektive med henblik på at være effektive – de bør selv kunne definere deres

prioriteter og kunne starte sager af egen drift uanset forpligtelserne til samarbejde, gensidig bistand og sammenhæng.

Artikel 29-gruppen har herefter forslag om opblødning af formuleringer med henblik på at overlade mere til tilsynsmyndighedernes egen bestemmelse. Datatilsynet kan tilslutte sig Artikel 29-gruppens synspunkter.

Hvis tilsynsmyndigheden skal kunne udnytte sine ressourcer bedst muligt, bl.a. for at tilgodese hensynet til flest mulig borgere, er det efter Datatilsynets opfattelse nødvendigt, at retsgrundlaget giver tilsynsmyndighederne den fornødne fleksibilitet og mulighed for prioritering i forhold til den konkrete opgavevaretagelse.

3.17.2. Hvad angår bestemmelserne om bøder har Artikel 29-gruppen ligeledes (s. 24) et ønske om, at tilsynene får et manøvrerum ("a margin of discretion"), når de beslutter sig for at pålægge en bøde. Datatilsynet er enig heri.

Under alle omstændigheder vil den foreslåede forpligtelse for tilsynet til at udstede administrative bøder og formentlig varetage opfølgningen heraf nødvendiggøre dedikerede personaleressourcer til håndhævelsesopgaver, jf. herved også tilsynets udtalelse af 12. marts 2012.

3.17.3. Tilsynet bemærker, at selv om forslaget afskaffer den hidtil kendte anmeldelsespligt, indebærer forslaget en række bestemmelser (jf. artikel 34) om pligt til forudgående godkendelse fra eller forudgående høring af tilsynsmyndigheden. Dette gælder bl.a. i forhold til visse tredjelandsoverførsler.

Datatilsynet opfordrer til, at man i det videre arbejde med disse regler har princippet om "accountability" i fokus, og at man fra dansk side arbejder for ikke at bebyrde virksomheder og myndigheder unødigt, herunder f.eks. ved at udvide forpligtelsen til at forelægge sager for tilsynet, f.eks. i forbindelse med internationale dataoverførsler.

3.18. Formaliseret samarbejde mellem datatilsynene
Der lægges i forslagets artikel 55 op til, at tilsynene skal udføre aktiviteter på anmodning fra et andet tilsyn.

Bestemmelsen i artikel 56 indebærer, at tilsynene skal gennemføre fælles undersøgelsesopgaver, fælles håndhævelsesforanstaltninger og andre fælles aktiviteter.

Det er Datatilsynets erfaring, at aktiviteter af denne karakter er meget ressourcekrævende. Tilsynet finder derfor, at det nøje bør overvejes, hvilke fælles aktiviteter der skal være tale om, og hvilket omfang aktiviteterne skal have.

3.19. Sammenhængsmekanismen
3.19.1. I en række tilfælde vil de nationale datatilsyn ikke kunne træffe afgørelse eller give bindende retningslinjer uden forinden at have iagttaget regler-

ne om sammenhængsmekanisme, som involverer forelæggelse for Det Europæiske Databeskyttelsesråd (i det følgende databeskyttelsesrådet).

Dette gælder dels de i artikel 58, stk. 2, nævnte tilfælde, dels har enhver tilsynsmyndighed, databeskyttelsesrådet og Kommissionen ret til at kræve en sag underlagt sammenhængsmekanismen. Databeskyttelsesrådet skal inden en uge beslutte, om det vil afgive udtalelse, og skal vedtage udtalelsen inden en måned. For Kommissionens adgang til at vedtage en udtalelse om de sager, som er rejst, gælder en 10-ugers frist (artikel 59), og i den periode må den nationale tilsynsmyndighed tilsyneladende ikke træffe afgørelse i sagen.

3.19.2. Datatilsynet bemærker, at bestemmelserne i artikel 58 må antages at have et ganske bredt anvendelsesområde. Eksempelvis vedrører § 58, stk. 2, litra a) foranstaltninger, der skal have retsvirkning, og som "*omfatter behandlingsaktiviteter, der vedrører udbud af varer eller tjenester til registrerede i flere medlemsstater eller overvågning af deres adfærd.*"

Danske virksomheder må antages at udbyde varer og tjenester til registrerede i flere medlemsstater. Datatilsynet går endvidere ud fra, at dette også kan forekomme hos offentlige myndigheder, hvis de udformer løsninger til betjening af personer bosat uden for Danmark, eksempelvis inden for beskæftigelses- og udlændingeområdet.

Datatilsynet kan oplyse, at det svenske datatilsyn på baggrund af en analyse af sine egne sager i 2011 skønner, at det totalt for EU kan handle om op til 1.500 sager om året, som vil være omfattet af reglerne om sammenhængsmekanisme.

Datatilsynet skal generelt opfordre til, at reglerne om Det Europæiske Databeskyttelsesråd overvejes nærmere i det videre arbejde, herunder hvilke sagstyper og spørgsmål der skal være omfattet af sammenhængsmekanismen, og hvilken rolle og kompetence Kommissionen skal have. Det forekommer således vidtgående, hvis Datatilsynets behandling af spørgsmål vedrørende internettjenester og -handel mv. skal være omfattet af denne mekanisme, og Kommissionen får beføjelse til at suspendere tilsynsmyndighedens foreslåede foranstaltning med den konsekvens, at tilsynet ikke må gennemføre foranstaltningen.

3.19.3. De i artikel 58, stk. 2, angivne frister på henholdsvis en uge for databeskyttelsesrådets beslutning om at afgive udtalelse og en måned for databeskyttelsesrådets vedtagelse af selve udtalelsen er efter Datatilsynets opfattelse meget korte. Dette skal ses i sammenhæng med, at en del af sagerne må antages også at rumme vanskelige vurderinger og kræve oversættelse af relevante dokumenter samt det forhold, at koordinering af fælles afgørelser mellem et større antal tilsynsmyndigheder i sig selv er en vanskelig proces.

Det forekommer Datatilsynet urealistisk, at databeskyttelsesrådet og de deltagende tilsynsmyndigheder på forsvarlig vis skal kunne håndtere alle de sager, som vil skulle forelægges, inden for de opstillede frister.

Som deltager i databeskyttelsesrådet må Datatilsynet for sit eget vedkommende udtrykke bekymring for, hvilke ressourcer det vil kræve at skulle deltage på kvalificeret vis i det fælles arbejde.

3.20. Det Europæiske Databeskyttelsesråd – organisering mv.
Datatilsynet bemærker, at databeskyttelsesrådet ikke kun består af de uafhængige datatilsyn, men også af en repræsentant fra Kommissionen. Databeskyttelsesrådets formand skal omgående underrette Kommissionen om alle aktiviteter i databeskyttelsesrådet, og Kommissionen får ret til at anmode databeskyttelsesrådet om at udføre opgaver og kan sætte frister for, hvornår databeskyttelsesrådet skal yde rådgivning efter anmodning fra Kommissionen, jf. artikel 66.

Som nævnt ovenfor finder Datatilsynet, at der er grund til at overveje Kommissionens rolle nærmere. Koordineringsprocedurerne – de såkaldte sammenhængsmekanismer – må efter Datatilsynets opfattelse indrettes således, at det alene er de uafhængige datatilsyn, som sikrer den ensartede anvendelse af reglerne.

Herudover er der efter Datatilsynets opfattelse behov for at overveje databeskyttelsesrådets kompetencer i forhold til de nationale datatilsyns kompetencer og i forhold til adgangen til at indbringe Datatilsynets afgørelser for domstolene efter grundlovens § 63.

Det samme gælder spørgsmålet om, hvordan national lovgivning på forskellige områder skal håndteres i forbindelse med sammenhængsmekanismen og databeskyttelsesrådet. Der henvises herved også til Artikel 29-gruppens udtalelse, s. 21.

3.21. Klageadgang og retsmidler over for nationale tilsynsmyndigheder
Forslagets artikel 73 indeholder regler om klageadgang til tilsynsmyndigheden. Som påpeget af Artikel 29-gruppen, jf. udtalelsen s. 21, forekommer det ikke hensigtsmæssigt, at registrerede og organer, sammenslutninger m.v. kan indgive klage i enhver medlemsstat. Datatilsynet finder, at det bør afgrænses nærmere i selve forordningen, hvilken tilsynsmyndighed en klage indgives til.

Forslaget indeholder også bestemmelser, som giver den registrerede mulighed for at gøre retsmidler gældende over for nationale tilsynsmyndigheder (artikel 74).

Datatilsynet finder, at den foreslåede bestemmelse i artikel 74. stk. 2, er vidtgående i forhold til at regulere tilsynsmyndighedens sagsbehandling, arbejdstilrettelæggelse og nødvendige prioritering af sager, der erfaringsmæssigt er af vidt forskellig karakter. Datatilsynet mener, at bestemmelsen bør overvejes nøje i det videre forløb.

Det samme gælder forslagets artikel 74, stk. 4, hvor der lægges op til, at hvis en registeret berøres af en afgørelse fra en tilsynsmyndighed i en anden med-

lemsstat, kan den registrerede anmode tilsynsmyndigheden i sin opholdsstat om at lægge sag an mod den tilsynsmyndighed, der i første omgang har truffet afgørelsen. Datatilsynet kan hermed henvise til de synspunkter, som fremgår af Artikel 29-gruppens udtalelse, s. 25.

3.22. Udstedelse af delegerede retsakter
I forslaget tillægges Kommissionen i flere bestemmelser kompetence til at vedtage såkaldte delegerede retsakter.

Efter Datatilsynets opfattelse må det tages i betragtning, at selv om Kommissionen er uafhængig i forhold til medlemsstaterne, er Kommissionen ikke en uafhængig databeskyttelsesmyndighed.

Databeskyttelseslovgivningen er indrettet med kompetence hos en række uafhængige datatilsyn, hvorved området adskiller sig væsentligt fra andre områder, hvor der er tillagt Kommissionen centrale kompetencer.

Tilsynet skal derfor opfordre til, at det for hvert punkt, hvor Kommissionen tillægges kompetence, overvejes, om dette er hensigtsmæssigt.

I den forbindelse må det bl.a. tages i betragtning, at delegerede retsakter i traktatens[2] artikel 290 er beskrevet som ikke-lovgivningsmæssige retsakter, der udbygger eller ændrer visse ikke-væsentlige elementer i den lovgivningsmæssige retsakt.

Tilsynets vurdering er, at en række af de områder, hvor der efter forslaget tillægges kompetence til at udstede delegerede retsakter, på ingen måde kan anses for ikke-væsentlige. Der er tale om områder, hvor der jævnligt fastsættes retningslinjer nationalt, enten i form af bestemmelser i særlovgivning, der præciserer i forhold til persondatalovens overordnede regler, eller som led i Datatilsynets praksis.

4. Forholdet mellem forordningen og gældende regler
4.1. Justitsministeriet har anført i grundnotatet, at forordningsforslaget berører forhold, der har relevans for en række retsområder.

Det fremgår endvidere, at en konsekvens af forslaget bl.a. vil være, at den regulering, der følger af lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven) – samt andre love, bekendtgørelser mv., der vedrører behandling af personoplysninger – efter omstændighederne vil skulle ophæves eller ændres i overensstemmelse med ordlyden af den endelige forordning.

I grundnotatet bemærkes det samtidig, at forordningsforslaget indeholder en række bestemmelser, hvorved medlemsstaterne på konkrete områder overlades beføjelse til – under overholdelse af forordningen – at fastsætte nærmere

[2] Traktaten om Den Europæiske Unions Funktionsmåde

regler om behandling af personoplysninger, jf. bl.a. pkt. 2.10 i grundnotatet, som omhandler forordningens kapitel IX.

I kapitel IX findes en bestemmelse, som giver medlemsstaterne adgang til under visse betingelser f.eks. at fastsætte regler om behandling af personoplysninger om helbredsforhold til brug for patientbehandling eller for historiske, statistiske eller videnskabelige forskningsformål.

Kapitlet indeholder endvidere regler om medlemsstaternes adgang til – under overholdelse af forordningen – at vedtage specifikke bestemmelser om behandling af personoplysninger i forbindelse med ansættelsesforhold og regler om behandling af personoplysninger til historiske, statistiske eller videnskabelige forskningsformål.

Herudover indeholder kapitlet en bestemmelse om, at medlemsstaterne – under overholdelse af forordningen – kan vedtage specifikke regler om forholdet mellem tilsynsmyndighedernes undersøgelsesbeføjelser og nationale tavshedspligtsregler.

Endvidere indeholder kapitlet en bestemmelse om kirkers og religiøse sammenslutningers adgang til at opretholde gældende regler af omfattende karakter om behandling af personoplysninger under forudsætning af, at reglerne bringes i overensstemmelse med forslaget.

Den endelige fastlæggelse af, hvilke love der vil være behov for at ophæve eller ændre, vil ifølge grundnotatet finde sted i samarbejde med de berørte ressortministerier.

4.2.1. Datatilsynet bemærker, at der også i selve persondataloven er etableret særlig national regulering. Det gælder f.eks. vedrørende kreditoplysningsbureauer, retsinformation, forskning og statistik, personnumre og behandling af personoplysninger i optagelser fra tv-overvågning.

Datatilsynet har endvidere i forbindelse med høringer over lovforslag og bekendtgørelser gennem årene set et ganske stort antal bestemmelser i anden lovgivning, som i forhold til persondatalovens regler fraviger eller præciserer mulighederne for at behandle personoplysninger.

Hertil kommer de gældende (og kommende) EU-retsakter, hvor der forekommer fravigelser i forhold til såvel persondataloven som databeskyttelsesdirektivet. Eksempelvis har tilsynet for nylig besvaret en høring om et forslag til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked. Heri indeholder en artikel (artikel 15) selvstændige sikkerhedskrav, og Datatilsynet har opfordret til, at det afklares, om denne træder i stedet for sikkerhedskravene efter persondataloven og på sigt det kommende retsgrundlag for databeskyttelse.

4.2.2. I en del af de danske love, hvor der ændres eller præciseres i forhold til persondataloven, sker dette netop som led i gennemførelse af EU-lovgivning.

Datatilsynet skal derfor pege på, at der kan være behov for også at afklare forholdet mellem forordningen og anden EU-regulering, herunder såvel forordninger som direktiver og de nationale love, der gennemfører disse.

4.2.3. Hvad angår de danske særlovbestemmelser, der ikke gennemfører EU-lovgivning, kan bl.a. nævnes en række hjemler til kontrolsamkøring, til offentliggørelse af kontrolresultater og til videregivelse af oplysninger i forbindelse med digitale løsninger.

En stor del af de danske særbestemmelser må antages at være præciseringer, der er foretaget inden for rammerne af databeskyttelsesdirektivet.

Fordelen ved sådanne regler kan være dels at fastslå, at en behandling kan ske, således at brugerne ikke er henvist til at fortolke de generelle regler i persondataloven i deres daglige administration, dels at fastslå, at en given databehandling ikke bare kan ske, men *skal* ske, f.eks. en pligtmæssig videregivelse af personoplysninger.

Samtidig kan udtrykkelige bestemmelser i love og bekendtgørelser give større gennemsigtighed i forhold til de registrerede. Medfører en bestemmelse således en tilstrækkelig forudsigelighed for borgeren med hensyn til, at der vil ske en given behandling af oplysninger om den pågældende, kan dette overflødiggøre den individuelle underretning, som ellers kræves efter persondatalovens regler om oplysningspligt.

Datatilsynet finder, at der så tidligt som muligt – og før den danske holdning til forordningsforslaget endeligt fastlægges – bør foretages en grundig analyse af forholdet til anden lovgivning.

5. Afsluttende bemærkninger

Som nævnt indledningsvis synes yderligere analyse og afklaring nødvendig for at fastlægge det præcise indhold af forslagets mange og detaljerede bestemmelser. Datatilsynet bidrager gerne hertil i det videre forløb.

Med hensyn til de økonomiske konsekvenser af den fremsatte reformpakke på databeskyttelsesområdet uddyber Datatilsynet gerne den foreløbige vurdering, som tilsynet gav i udtalelsen af 12. marts 2012.

Med venlig hilsen

Janni Christoffersen
Direktør

atp=

Justitsministeriet
Slotsholmsgade 10
1216 København K

jm@jm.dk

6. juli 2012

Ref. nr. ATP-01-05-13

ATP
Kongens Vænge 8
3400 Hillerød

Tlf.: 48 20 49 14
Fax: 48 20 48 00
www.atp.dk
CVR-nr.: 43405810

Telefontid:
Man-fre: 8.00-21.00

Høring vedrørende Kommissionens forslag til generel forordning om databeskyttelse, j.nr. 2012-3756-0005

Justitsministeriet har den 16. maj 2012 fremsendt Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og den fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

ATP er generelt positiv over for, at Kommissionen med forslaget søger yderligere at beskytte fysiske personers grundlæggende ret til beskyttelse af personoplysninger og samtidig fokuserer på at sikre et ensartet databeskyttelsesniveau for fysiske personer i hele EU.

ATP hilser det velkomment, at beskyttelsen af personoplysninger forbedres i takt med, at omfanget af datadeling og –indsamling stiger som konsekvens af de øgede teknologiske muligheder.

ATP finder imidlertid, at en række af forordningsforslagets bestemmelser rejser en række ubesvarede spørgsmål og rummer uklarheder i forhold til deres rækkevidde og nærmere indhold, som bør søges afklaret, ligesom en række bestemmelser bør tilpasses den offentlige forvaltnings virkelighed.

ATP finder endvidere ikke umiddelbart, at forordningsforslaget skaber den rette balance mellem hensynet til databeskyttelse og andre væsentlige hensyn, herunder navnlig til den offentlige sektors effektive opgaveløsning og til udnyttelsen af de muligheder, som moderne teknologi medfører.

Generelt støtter ATP derfor, at det sikres – som også bemærket i Justitsministeriets grundnotat – at forordningsforslaget rammer en passende balance mellem den merværdi, som den øgede og ensartede beskyttelse af personoplysninger medfører, og de omkostninger, som forslaget vil påføre de dataansvarlige.

Kort om ATP Koncernens administrationsaktivitet

ATP Koncernen er Danmarks største pensions- og sikringsselskab. Koncernens aktiviteter kan inddeles i fire virksomheder, som arbejder med henholdsvis pension,

afdækning, investering og administration.

Kernen i ATP's virksomhed er at levere sikre og forudsigelige pensioner til medlemmerne. ATP forvalter mere end 500 milliarder kroner af danskernes opsparede pensionsmidler og afkastet heraf anvendes til løbende udbetalinger af livslang pension til de 838.000 medlemmer, der ved udgangen af 2011 modtog denne samt hensættelser til fremtidige pensioner og udbetaling af pensionsafkastskat. Fondsanbringelse via investerings- og afdækningsvirksomheden er et middel til at betjene denne del af ATP's opgaver.

Særligt ATP Koncernens administrationsaktivitet giver i det følgende anledning til bemærkninger i forhold til Kommissionens forslag: ATP er oprettet ved lov[1] og har status som særlig forvaltningsenhed. ATP er dermed ikke en statslig myndighed eller en del af statsforvaltningen, men er en del af den offentlige forvaltning.

ATP administrerer en række lovbundne ordninger, hvis karakteristika er, at de har til formål at sikre grundlæggende økonomisk tryghed for borgerne.

ATP er aktuelt tillagt administration og drift af følgende ordninger:

- ATP Livslang Pension – obligatorisk pensionsopsparing for lønmodtagere.
- AER (Arbejdsgivernes Elevrefusion) – udbetaler støtte for at skabe flere praktikpladser inden for erhvervsuddannelserne.
- AES (Arbejdsmarkedets Erhvervssygdomssikring) - udbetaler erstatninger til lønmodtagere med en anerkendt erhvervssygdom.
- Barsel.dk - lovbestemt barselsordning for arbejdsgivere på det private arbejdsmarked
- DA-Barsel - overenskomstbestemt barselsordning for virksomheder, der er organiseret under Dansk Arbejdsgiverforening (DA).
- Feriekonto - administrerer feriepenge for lønmodtagere, der ikke er omfattet af en feriekortordning.
- LG – Lønmodtagernes Garantifond. Sikrer, at lønmodtagere får udbetalt løn, feriepenge, pension og løntillæg, hvis arbejdsgivere går konkurs eller ophører og er ude af stand til at betale.
- SFS – Skattenedslag for seniorer. Nedslag i skat til seniorer, der arbejder.
- SUPP – Supplerende arbejdsmarkedspension for førtidspensionister.

[1] ATP-loven, jf. lovbekendtgørelse nr. 942 af 2. oktober 2009.

- Udbetaling Danmark - Myndigheden Udbetaling Danmark overtager i efteråret 2012 en række opgaver fra kommunerne. ATP skal drive den nye myndighed. Udbetaling Danmark får ansvar for udbetaling af offentlige ydelser i størrelsesordenen 180 milliarder årligt i sager om folkepension, dele af førtidspension, boligstøtte, børne- og ægtefællebidrag, børnetilskud, børne- og ungeydelse og barselsdagpenge.

ATP administrerer således en bred vifte af opgaver, der indebærer, at ATP behandler – som dataansvarlig eller som databehandler – en større mængde personoplysninger om borgerne i Danmark fra fødsel til død, såvel stamdata som – om end i mindre grad – følsomme oplysninger.

Kendetegnende for ovennævnte ordninger er, at administrationen og driften varetages på omkostningsdækket basis. Dette indebærer, at ATP ikke kan påregne en avance i forbindelse med administration og drift. Dette indebærer endvidere, at de afkast, som opnås i afdæknings- og investeringsvirksomheden anvendes til løbende udbetalinger eller hensættelser til fremtidige udbetalinger til borgerne.

En del af virksomheden bliver herudover drevet på kommercielle vilkår. Gennem datterselskabet ATP PensionService A/S ydes pensionsadministration.

Specifikke bemærkninger til forordningsforslaget

Artikel 7 – samtykkekravet

For så vidt angår samtykkekravet i forordningsforslagets artikel 7 fremgår det af stk. 4, at samtykke ikke tilvejebringer et retsgrundlag, "hvis der er en klar skævhed mellem den registrerede og den registeransvarlige". ATP ser intet behov for en nærmere præcisering af samtykkebegrebet. For så vidt angår dette nye kriterium lægges det til grund, at skævheden, som ikke er udtømmende defineret, ikke omfatter de tilfælde, hvor en borger får behandlet en sag i den offentlige forvaltning med henblik på at få udbetalt en ydelse.

I de tilfælde, hvor det offentlige af økonomiske hensyn fastlægger en digital kommunikationsvej med borgeren i sager, hvor borgeren ansøger om en ydelse eller sikring, bør sagstypen ikke i sig selv medføre en skævhed mellem parterne, som kan hindre det offentliges bestræbelser på at effektivisere ansøgningsprocesser og optimere brugervenlighed.

Artikel 12 – procedurer for udøvelsen af den registreredes rettigheder

Det fremgår af forordningsforslagets artikel 12, stk. 4, at meddelelser og handlinger, der iværksættes i medfør af stk. 1, er gratis. ATP ønsker at rette opmærksomheden på de administrative omkostninger, der kan være forbundet med en registrerets udøvelse af sin ret til eksempelvis indsigt og henviser til bemærkningerne nedenfor vedrørende artikel 15 og 18 om et enkelt og billigt elektronisk format.

Det fremgår endvidere af artikel 12, stk. 6, at Kommissionen kan fastlægge standardformularer og –procedurer. ATP skal derfor opfordre til, at eventuelle konkrete, harmoniserede standarder for meddelelse af indsigt sendes i høring af Kommissionen.

Artikel 14 – oplysningspligten

ATP noterer sig, at oplysningspligten i medfør af forordningsforslaget udvides i forhold til det gældende i og med, at eksempelvis oplysninger om det tidsrum, hvori oplysninger bevares, nu skal indgå.

ATP opbevarer oplysninger i tidsrum, der kan variere efter hvilken ordning, en borger er omfattet af. En redegørelse for, hvor længe oplysninger opbevares, vil derfor forudsætte en udvidelse af ATPs forpligtelser i den henseende med deraf følgende administrative omkostninger.

Kommissionen tillægges i artikel 14, stk. 7 og 8 retten til at fastlægge nærmere retningslinjer, herunder fastsætte procedurer og formularer og ATP skal opfordre til, at eventuelle konkrete tiltag sendes i høring af Kommissionen.

Artikel 15 – retten til indsigt

For så vidt angår forordningsforslagets artikel 15 om retten til indsigt noterer ATP, at Kommissionen i stk. 4 gives mulighed for at fastlægge standardprocedurer og –formularer for anmodning og meddelelse af adgang til oplysninger. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 87, stk. 2.

Det er væsentligt for en effektiv administration af de lovbundne ordninger, som ATP administrerer, at retten til indsigt i videst muligt omfang kan behandles ensartet for samtlige de anmodninger om indsigt, som ATP måtte modtage. I den forbindelse er et enkelt elektronisk format, som f.eks. nemt kan downloades via en selvbetjeningsløsning efter log-in med eksempelvis digital signatur en model, som vil kunne administreres enkelt og med lave omkostninger og kort sagsbehandlingstid.

Formatet bør være obligatorisk, således at en virksomhed eller institution kan indrette sine it-systemer på en forudsigelig model og administrere effektivt. ATP skal derfor opfordre til, at eventuelle konkrete, harmoniserede standarder for meddelelse af indsigt sendes i høring af Kommissionen.

Konkret foreslår ATP, at der fastsættes retningslinjer om udlevering af oplysninger i CSV-filer (comma-separated values), der er et simpelt tekstformat, som bruges i mange sammenhænge, hvor større mængder data skal flyttes fra én database til en anden og disse ikke er indbyrdes forbundne. En CSV-fil kan benyttes til edb-behandling hos modtageren. Materialet kan endvidere flyttes over til et excel-regneark og herefter gøres til genstand for sorteringer, udsøgninger og sammenlægninger etc.

Artikel 17 – retten til at blive glemt og ret til sletning

Det følger af forordningsforslagets artikel 17, stk. 1, litra a, at den registrerede kan kræve, at en dataansvarlig sletter personoplysninger om vedkommende, såfremt personoplysningerne ikke længere er nødvendigt til opfyldelse af de formål, hvortil de er blevet indsamlet eller på anden vis er blevet behandlet.

ATP ønsker at gøre opmærksom på, at der ved behandlingen af store mængder persondata på økonomisk og administrativt effektiv vis forudsættes visse automatiserede sletterutiner. Data slettes således for hele år ad gangen og inden for et enkelt år vil visse data kunne stamme fra først på året og dermed være næsten et år ældre end de sidste data fra det pågældende år.

ATP finder det problematisk, såfremt en registreret med forordningsforslaget opnår ret til at kræve individuel sletning hos en dataansvarlig uafhængigt af automatiserede og økonomisk samt administrativt hensigtsmæssige sletteprocedurer.

Artikel 18 – retten til dataportabilitet

Tilsvarende bemærkes det for så vidt angår forordningsforslagets artikel 18 om retten til dataportabilitet, at en sådan ret ikke bør medføre øgede omkostninger for den registeransvarlige i nævneværdig grad. En sådan ret bør derfor fastlægges på en sådan måde, at der fastlægges et enkelt format, som den registeransvarlige har ret til at udlevere i, eksempelvis CSV-filer jf. ovenfor.

Omkostninger til tilpasning til individuelle ønsker om data-formater, f.eks. udlevering på USB-nøgler, bør derfor undgås, da tilvejebringelse af eksempelvis USB-nøgler og lignende kan være bekosteligt og it-sikkerhedsmæssigt betænkeligt, hvor data skal modtages som følge af retten til dataportabilitet.

ATP skal påpege, at en registrerets brug af retten til dataportabilitet i de tilfælde, hvor en borger ønsker at levere en mængde data til ATP eller en af de ordninger, som ATP administrerer, vil medføre en ekstra administrativ byrde til gennemgang af data. ATP modtager i dag data til brug for administration af de lovbundne ordninger fra offentlige registre så som CPR-registret. Validiteten af disse data fra offentlige registre medvirker til, at ordningerne kan administreres hensigtsmæssigt, såvel i økonomisk som administrativ henseende.

Endvidere vil der potentielt kunne være en risiko for, at en registreret i forbindelse med udøvelsen af denne rettighed leverer flere data end den modtagende dataansvarlige har behov for at behandle til sit formål.

ATP skal derfor på tilsvarende vis som ved forordningsforslagets artikel 15 opfordre til, at eventuelle konkrete, harmoniserede standarder for dataportabilitet i artikel 18, stk. 3, sendes i høring af Kommissionen.

Artikel 20 – profilering

Forordningsforslagets artikel 20 om profilering er en nyskabelse i databeskyttelsesretlig henseende. Det følger af forslaget, at enhver fysisk person har ret til ikke at være genstand for en foranstaltning, der har retsvirkning for vedkommende, eller som berører vedkommende i væsentlig grad, og som er baseret alene på automatisk databehandling, der har til formål at vurdere bestemte personlige forhold.

ATP ønsker at rette opmærksomheden på, hvorvidt dansk lovgivning i den henseende har den fornødne udtrykkelighed eller om forordningsforslaget vil indebære et behov for præcisering af en række lovbestemmelser.

Det bør endvidere sikres, at forordningsforslaget ikke unødigt hindrer en økonomisk og effektiv løsning af væsentlige opgaver i den offentlige forvaltning. Eksempelvis "objektiveret sagsbehandling", hvor moderne teknologi anvendes til at automatisere og dermed effektivisere masseafgørelser om eksempelvis tildeling af ydelser på baggrund af lov eller i henhold til lov fastlagte, objektive kriterier. Denne automatisering vil endvidere kunne benyttes til at sikre en mere ensartet sagsbehandling

Sikringen af en økonomisk effektiv løsning af offentlige opgaver i de kommende år forudsætter, at det bliver muligt at benytte de muligheder, som moderne teknologi tilbyder. Til illustration henvises til den aftale, som den tidligere regering og KL indgik i juni 2010 om at samle dele af den objektive sagsbehandling i en stordriftsorganisation fra efteråret 2012 (Udbetaling Danmark). Stordriftsorganisationen skal, efter en to-årig indfasning, spare kommunerne for knap 300 mio. kr. om året. Den enkelte kommune kan dermed tilgodese andre kommunale områder med de frigjorte midler.

Bestemmelser om administrative byrder for den dataansvarlige

ATP noterer sig, at forslaget vil medføre nye administrative byrder i form af øgede dokumentationskrav, herunder konsekvensanalyser i forordningsforslagets artikel 28 og 33, samt pligt til udpegning af en databeskyttelsesansvarlig, jf. forslagets artikel 35.

ATP ønsker i den henseende særligt at fremdrage forordningsforslagets artikel 31, der forudsætter anmeldelse af brud på persondatasikkerheden "uden unødig forsinkelse" og om muligt senest 24 timer efter, at sikkerhedsbruddet er blevet den registeransvarlige bekendt.

Den foreslåede tidsfrist for anmeldelse og pligten til begrundelse for senere anmeldelser stiller store krav til identificeringen af et sikkerhedsbrud og opfølgningsplaner herfor. ATP vil henstille til, at formuleringen af forordningsforslaget i stedet prioriterer, at der senest 24 timer efter et brud på persondatasikkerheden skal være påbegyndt afhjælpning.

Endelig rummer forordningsforslagets artikel 79 om administrative sanktioner et bødeniveau, som må betegnes som en væsentlig nyskabelse på området. ATP finder generelt, at bødeniveauet bør overvejes i relation til proportionalitetsprincippet og

henviser i øvrigt til, at det vil være af afgørende betydning, hvorledes virksomhedsbegrebet afgrænses i forordningen.

Selvejende institutioner, som ATP, der udgør en del af den offentlige forvaltning og administrerer lovbundne ordninger på omkostningsdækket basis vil for så vidt angår den administrative del af virksomheden ikke have en årlig omsætning. Eventuelle sanktioner vil derfor alene kunne pålægges, hvis midlerne tages fra de pensions- og sikringsordninger, som administreres på vegne af borgerne.

På denne baggrund vurderes det nødvendigt i det videre arbejde med forordningsforslaget at gøre udtrykkeligt op med arten af de administrative sanktioner, som kan tillægges offentlige myndigheder og den offentlige forvaltning i sin helhed.

Det bør i den forbindelse efterstræbes, at virksomheder som ATP, der udøver sine aktiviteter på baggrund af lov og i samfundsøjemed ikke kan ifalde administrative bøder eller at det efterstræbes, at der ved fastlæggelsen af størrelsen af de administrative sanktioner tages behørigt hensyn til de særlige forhold, der gør sig gældende for virksomheder som ATP.

Venlig hilsen

Marlene Wiese Svanberg

Advokatrådet

ADVOKAT SAMFUNDET

Justitsministeriet
Slotsholmsgade 10

1216 København K

jm@jm.dk

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98
FAX 33 36 97 50

DATO: 5. juli 2012
SAGSNR.: 2012 - 1662
ID NR.: 185836

Høring - over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

Ved e-mail af 11-05-2012 har Justitsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte forslag.

Advokatrådet har følgende bemærkninger:

1. Generelle bemærkninger vedrørende forordningen, herunder valg af retsakt

Formålet med den fremtidige persondataregulering er ifølge Europa-Kommissionens forslag dels beskyttelse af fysiske personers grundrettigheder, herunder retten til beskyttelse af personoplysninger, dels sikring af en fri udveksling af persondataoplysninger i EU. Formålet med forslaget er således det samme som formålet bag persondatadirektivet, der vil blive ophævet og erstattet med den endelige forordning.

Retssikkerhedsmæssigt vil forordningen for en umiddelbar betragtning formentlig medføre en række forbedringer, men i forhold til gældende danske regler vil der også være en række områder, hvor forordningen vil yde danske borgere en ringere retssikkerhed. Dette skal sammenholdes med og opvejes mod, at forordningen utvivlsomt vil lægge større administrative byrder på såvel myndigheder som danske virksomheder, herunder især mellemstore og mindre virksomheder, som kun har tilstedeværelse i et land i EU. Advokatrådet finder, at det i den nuværende økonomiske situation bør overvejes, om det er hensigtsmæssigt at belaste virksomheder med regler, som kræver et sådant øget ressourceforbrug.

Forordningen lægger endvidere op til, at Kommissionen i betydeligt omfang er tillagt bemyndigelse til at udfylde og supplere forordningens generelle regler gennem delegerede retsakter og gennemførelsesretsakter. Advokatrådet vurderer, at dette indebærer en risiko for, at udfyldningen af de retlige standarder i nogle tilfælde ikke

vil forekomme naturlige, rimelige og tilstrækkelig fleksible i forhold til gældende nationale normer og traditioner. Der henvises til afsnit 2.22 nedenfor.

Forordningsforslaget indeholder 26 delegationsbestemmelser, og selvom der også er udstedt enkelte bekendtgørelser med hjemmel i persondataloven, må det endvidere antages, at virksomheder vil skulle administrere et langt større regelgrundlag, end hvad nu er tilfældet. Dette vil som nævnt navnlig medføre en øget administrativ byrde for små og mellemstore virksomheder, som ikke drager samme fordel af harmoniseringen, som virksomheder repræsenteret i flere EU-lande.

Det skal i den forbindelse fremhæves, at det forekommer vidtgående, at Kommissionen tillægges kompetence til at udfylde interesseafvejningsreglen (artikel 6 stk. 1 nr. f), og at interesseafvejningsreglen – som i vidt omfang har bidraget til at gøre området operationelt – helt afskaffes som hjemmelsgrundlag indenfor den offentlige forvaltning. Advokatrådet vurderer, at en sådan afskaffelse vil give en del udfordringer i forhold til gældende praksis, idet interesseafvejningsreglen anvendes som hjemmelsgrundlag på mange områder, herunder i forbindelse med videregivelse, offentliggørelse på internettet mv. Advokatsamfundet opfordrer til, at hensigtsmæssigheden af ovenstående overvejes meget nøje.

Kommissionens målsætning er en mere uniform anvendelse og håndhævelse af persondatabeskyttelsesreglerne i hele EU, hvilket valget af retsakt også afspejler. Retsområdet er dog og vil forsat være kendetegnet af mange generelle regler og retlige standarder, der skal udfyldes i praksis. Selv i dag er det gældende regelsæt vanskeligt at forstå og at håndtere i praksis. Samtidig berører persondataretten i takt med udbredelsen af den elektroniske kommunikation og sagsbehandling i stadig stigende omfang virksomheder og personer. Behovet for et smidigt tilsyn, der kan agere forholdsvist hurtigt, må derfor formodes at blive endnu vigtigere, end det allerede er i dag. Et nationalt tilsyn kombineret med den nuværende artikel 29-gruppe – eventuelt i en styrket form med tilførsel af yderligere ressourcer - der løbende fremkommer med vejledende udtalelser for hele EU, forekommer derfor at være et mere velegnet og smidigt system til på sigt at udvikle retsområdet og opnå større retsenhed i EU.

Nedenfor følger bemærkninger til en række af forslagene i forordningen.

2. Bemærkninger til forslag i forordningen

2.1 Territorialt anvendelsesområde

Forordningsudkastet, jf. artikel 3, omfatter som noget nyt dataansvarlige, der ikke er etableret i Danmark eller EU, når de behandler oplysninger om personer bosiddende i EU, f.eks. i forbindelse med udbud af varer eller tjenester.

Advokatrådet finder, at der er tale om en meget bred bestemmelse, og at der som minimum er behov for, at forordningen også regulerer, hvordan bestemmelsen skal kunne håndhæves i praksis overfor virksomheder i tredjelande.

2.2 Registerbegrebet
I forarbejderne til persondataloven er det præciseret, at manuelle akter, som indgår i den dataansvarliges konkrete sagsbehandling, mapper med sagsakter eller samlinger af sådanne mapper, ikke er omfattet af registerbegrebet, selvom de måtte være struktureret efter bestemte kriterier.

Af forordningens betragtning 13 fremgår, at beskyttelsen af fysiske personer bør være teknologineutral og ikke afhænge af den anvendte teknik, og at beskyttelsen skal finde anvendelse både på elektronisk og manuel behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Advokatrådet vurderer, at anvendelsesområdet for forordningen lægger op til også at omfatte manuelle akter, som indgår i den dataansvarliges konkrete sagsbehandling, hvilket vil indebære en udvidelse af anvendelsesområdet.

I forhold til persondataloven vil dette i så fald indebære en udvidelse af anvendelsesområdet for loven, f.eks. til at omfatte manuelle papirbaserede sager hos både virksomheder og myndigheder. For borgerne vil det betyde, at området for indsigtsret og retten til at modtage oplysninger udvides og dermed bidrage til en øget retssikkerhed, men udvidelsen vil også kræve, at virksomheder og myndigheder skal anvende flere ressourcer. Advokatsamfundet skal opfordre til at det søges afklaret, om en sådan udvidelse alt taget i betragtning er hensigtsmæssig.

2.3 Reglen i persondatalovens § 1, stk. 2, forsvinder
Det følger af persondataloven § 1, stk. 1, at loven gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Denne bestemmelse er suppleret af persondataloven § 1, stk. 2, hvorefter loven gælder for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden.

Bestemmelsen i persondataloven § 1, stk. 2, følger ikke af det bagvedliggende direktiv (95/46/EF) og er således en særegen regel for Danmark. Bestemmelsen indebærer, at eksempelvis fysiske samlinger af personalemapper, af ansøgninger fra jobansøgere og af mødereferater med oplysninger om identificerbare medarbejdere falder inden for lovens område. Dette ville ikke være tilfældet uden stk. 2, idet sådanne samlinger ikke eller i hvert fald ikke altid antages at udgøre et "register" efter stk. 1.

Forslaget til forordning angiver samme materielle anvendelsesområde som persondatadirektivet og indeholder således ikke en regel svarende til persondataloven § 1, stk. 2. Forslaget indebærer derfor umiddelbart en forringelse af

persondatabeskyttelsen, idet beskyttelsen ikke længere vil omfatte eksempelvis en samling af personalemapper. Det kan dog ikke afvises, at "register" vil blive fortolket bredere af EU-Domstolen og således omfattende eksempelvis personalemapper.

Advokatrådet foreslår derfor, at det eksempelvis i forordningens indledende betragtninger (præamblen) afklares om et "register" også omfatter en fysisk samling af personalemapper og lignende.

2.4 Samtykke vil ikke længere kunne udgøre behandlingsgrundlag
Efter gældende ret er samtykke kun gyldigt som behandlingsgrundlag, hvis der er tale om et reelt frivilligt samtykke. Der kan således være situationer, hvor den registrerede er under et så stort pres fra den dataansvarlige, at der ikke kan siges at foreligge et reelt frivilligt samtykke. Det er dog i dansk ret antaget, at den omstændighed, at der er tale om et ansættelsesforhold - og således et vist afhængighedsforhold - ikke i sig selv indebærer, at et samtykke er ufrivilligt. Det er endvidere antaget, at den omstændighed, at en person giver et samtykke for at opnå en eller anden modydelse, f.eks. et job eller for ikke at blive afskediget, ikke betyder, at samtykket er ufrivilligt.

I forordningsforslaget, jf. artikel 7, lægges der op til, at samtykke ikke kan anvendes som behandlingsgrundlag i ansættelsesforhold, idet det fremgår af betragtning 34:

"Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context."

Der er således angiveligt tale om en ophævelse af arbejdsgiverens adgang til at benytte samtykke som databehandlingsgrundlag. Dette vil formentlig indebære en væsentlig administrativ byrde for arbejdsgiveren, idet arbejdsgiveren ved hver behandling af almindelige persondata vil skulle vurdere konkret, om behandlingen falder ind under et af de andre (mere afvejningsbetingede) databehandlingsgrundlag.

I forhold til behandling af følsomme persondata, er det ikke ualmindeligt, at medarbejderen af egen drift oplyser arbejdsgiveren om f.eks. helbredsmæssige forhold i forbindelse med sygdom. Efter gældende ret vil behandlingsgrundlaget for denne indsamling være samtykke, idet medarbejderen ved selv at have afgivet oplysningerne i sagens natur har samtykket til arbejdsgiverens viden om de helbredsmæssige forhold.

Efter forordningen vil arbejdsgiveren dog ikke kunne anvende samtykke som behandlingsgrundlag, og der vil næppe kunne findes andet anvendeligt behandlingsgrundlag for denne og lignende situationer. Arbejdsgiveren vil således have overtrådt forordningen, og selvom arbejdsgiveren - som følge af manglende forsæt/uagtsomhed - ikke kan pålægges bøde, forekommer dette ikke rimeligt.

Der er således tale om en ret indgribende ændring i retstilstanden for arbejdsgivere.

Hensynet til at undgå, at medarbejdere giver samtykke af frygt for konsekvenserne for forholdet til arbejdsgiveren, kunne varetages med mindre vidtgående foranstaltninger. Der kunne eksempelvis anvendes samme principper som kendes fra den udvidede beskyttelse i forbindelse med medarbejderes fremsættelse af krav om ligeløn. Hvis medarbejderen afviser at samtykke til den pågældende databehandling, kunne der opstilles en bevisregel, således at medarbejderen i en periode på (eksempelvis) seks måneder fra tidspunktet for denne afvisning opnår en udvidet bevismæssig beskyttelse mod afskedigelse og forringelse af ansættelsesvilkårene i øvrigt. Hvis medarbejderen afskediges i denne periode, ville det påhvile arbejdsgiveren at bevise, at afskedigelsen ikke helt eller delvist var begrundet i denne afvisning af at give samtykke.

2.5 Behov for klarlæggelse af muligheden for nationale regler og kollektive aftaler

Formålet med forordningen er som indledningsvist nævnt at totalharmonisere medlemsstaternes regulering af persondatabeskyttelse.

Forordningsforslaget ankerkender dog, at der på arbejdsmarkedet er særlige hensyn, der kan berettige visse nationale særregler. Der åbnes i forslagets artikel 82 op herfor.

Det fremgår af artikel 82, at medlemsstaterne kan fastsætte egne regler omkring en række forhold på arbejdsmarkedet, dog på den væsentlige betingelse, at der er tale om regler "[w]ithin the limits of this Regulation". Der synes således ikke at være mulighed for nationalt at fastsætte strengere regler, end de, som fremgår af forordningen. Endvidere fremgår det af artikel 82(3), at Kommissionen kan fastsætte nærmere krav til medlemsstaternes udnyttelse af denne mulighed.

Det bør efter Advokatrådets opfattelse tydeliggøres, hvilke muligheder for at gennemføre nationale særregler, der præcis ligger i artikel 82(1), og således hvad der nærmere forstås med "[w]ithin the limits of this Regulation".

Et meget væsentligt spørgsmål er også, i hvilket omfang forordningen tillader, at arbejdsmarkedets parter fortsat indgår kollektive aftaler om persondatabeskyttelse, idet der navnlig i samarbejdsudvalgssystemet behandles forhold omkring persondatabeskyttelse.
Artikel 82 vedrører efter sin ordlyd alene regler fastsat af medlemsstaterne ("Member States may adopt by law specific rules") og regulerer derfor ikke umiddelbart kollektive aftaler om persondatabeskyttelse. Forordningens totalharmoniserende formål taget i betragtning kan det dog ikke afvises, at det er Kommissionens hensigt, at det er det brede statsbegreb, der finder anvendelse, således at der ved "medlemsstat" forstås også faglige sammenslutninger, der fastsætter løn- og ansættelsesvilkår.[1]

[1] Sørensen og Nielsen: "EU-Retten", 5. udgave, DJØF (2010), side 268

Det følger af artikel 152 TEUF, at:
"Unionen anerkender og fremmer arbejdsmarkedsparternes rolle på EU-plan under hensyntagen til de nationale systemers forskelligartede karakter. Den letter dialogen mellem dem og respekterer deres uafhængighed."

Der er derfor traktatmæssig støtte – juridisk såvel som politisk – for, at der bør være adgang til kollektivt at aftale tilpasninger på området for persondatabeskyttelse. Advokatrådet skal pege på, at navnlig for arbejdstagersiden er det formentligt afgørende at bevare denne mulighed.

2.6 Børn
Forordningsforslaget har i artikel 8 fastsat særlige bestemmelser for behandling af personoplysninger om børn. Advokatrådet er overordnet set positiv overfor den yderligere styrkelse af børnenes retsstilling men har vanskeligt ved at se, hvordan den dataansvarlige skal indrette sine systemer for at kunne få et verificerbart samtykke.

2.7 Oplysninger om strafbare forhold
Advokatrådet vurderer, at der er behov for en klargøring af om artikel 9, stk. 2, giver virksomheder mulighed for at foretage behandling af strafbare oplysninger i samme omfang som i dag, f.eks. i forbindelse med whistleblowing-ordninger.

2.8 Retten til at blive glemt
Advokatrådet skal også hilse det velkomment, at der indføres regler, jf. artikel 17, om retten til at blive glemt, som en udvidelse reglerne om sletning.

2.9 Dataportabilitet
Forordningsudkastets artikel 18 indeholder en bredt formuleret ret til den registrerede til at få kopi af oplysninger, der er genstand for behandling, udleveret af den dataansvarlige. Advokatrådet formoder, at der ikke er tale om, at oplysningerne skal slettes hos den dataansvarlige, men skal opfordre til at det klargøres.

2.10 Datasikkerhed
Advokatrådet opfordrer til, at det nøje overvejes om systemet, jf. artikel 30, er hensigtsmæssigt ud fra en retssikkerhedsbetragtning. Henset til den hast, hvormed den elektroniske kommunikation udvikler sig, forekommer ikke hensigtsmæssigt, hvis nationale tilsyn fremover ikke har mulighed for at stille konkrete krav til datasikkerheden via henstillinger eller lign.

2.11 Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden
I relation til artikel 31, stk. 1, skal Advokatrådet opfordre til, at bestemmelsens fokus rettes mod, at virksomhederne først og fremmest skal tage aktion for at stoppe og på længere sigt at hindre sikkerhedsbrist, og at der sker en afklaring i forhold til reglerne om selvinkriminering. Anmeldelse til tilsynsmyndighederne bør endvidere kun ske ved alvorligere brist.

2.12 Konsekvensanalyse
Advokatrådet er positiv overfor forslagets bestemmelser i artikel 33 og 34, hvorefter der skal gennemføres en konsekvensanalyse vedrørende databeskyttelse, når der er tale om behandlingsformer, der kan indebære særlige risici, dog forudsat at der ikke kommer til at gælde en generel godkendelses- og anmeldelsesordning.

2.13 Databeskyttelsesansvarlige - en ny medarbejdergruppe med særlig beskyttelse
I medfør af forordningsudkastets artikel 35 skal alle offentlige myndigheder og virksomheder med flere end 250 ansatte udpege databeskyttelsesansvarlige, som skal medvirke til forordningens overholdelse.

Advokatrådet har erfaret, at ordninger med databeskyttelsesansvarlige i bl.a. Tyskland, Norge og Sverige er positive. Advokatrådet ser derfor positivt på den foreslåede ordning.

Advokatrådet skal fremhæve, at det fremgår af artikel 35(7), at den databeskyttelsesansvarlige nyder en væsentlig stillingsbeskyttelse: "During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties."

Da begrebet "dismissal" kan dække såvel afskedigelse som bortvisning, bør det præciseres, hvilke situationer, der er omfattet. Det forekommer i den forbindelse ikke rimeligt, hvis en arbejdsgiver er forhindret i at bringe ansættelsesforholdet til ophør som følge af væsentlig misligholdelse (bortvisning).

Endvidere bør der søges skabt klarhed omkring forholdet mellem de strafferetlige og civilretlige sanktioner for overtrædelse af bestemmelsen. Der bør således tages stilling til, om den pågældende kan kræve egentlig genansættelse, hvilket vil være atypisk i forhold til dansk ansættelsesret. Der kunne med fordel også i præamblen angives, om medlemsstaterne efter artikel 78 er forpligtede til at etablere et sanktionssystem i stil med det, der kendes fra området for ligebehandling og ikke-diskrimination. Ordlyden af artikel 78 kunne umiddelbart tyde på, at dette er tilfældet.

2.14 Øget ansvar til de dataansvarlige
I forordningens kapitel 4 om registeransvarlig og registerfører findes en række bestemmelser, som må antages at medvirke til en forbedret databeskyttelse, hvilket Advokatrådet bifalder.

2.15 Samarbejde mellem tilsynene mv. samt Datatilsynets øgede arbejdsopgaver
Der er i forordningsudkastet lagt op til, at de nationale tilsyn skal udføre opgaver efter anmodning fra andre tilsyn, samt at tilsynene skal udføre fælles undersøgelsesopgaver og aktiviteter, jf. artikel 55 og 56. Datatilsynets direktør skal endvidere have sæde i Det Europæiske Databeskyttelsesråd (Databeskyttelsesrådet).

Advokatrådet skal påpege, at disse aktiviteter, indberetningspligt i forbindelse med brug af hasteproceduren i artikel 61, udvidelsen af det geografiske anvendelsesområde, pligt til at anlægge sag efter artikel 74, stk. 4, hasteberedskab, anmeldelsesordningen for alle sikkerhedsbrist, mv. utvivlsomt vil nødvendiggøre, at Datatilsynet tilføres flere økonomiske ressourcer.

2.16 Sammenhængsmekanismen

I en række tilfælde vil de nationale datatilsyn ikke kunne træffe afgørelse eller give bindende retningslinjer uden forinden at iagttage reglerne om sammenhængsmekanisme, som involverer forelæggelse for Databeskyttelsesrådet.

I medfør af artikel 58, stk. 2, har Kommissionen ret til at kræve enhver sag underlagt sammenhængsmekanismen. Inden en uge skal Databeskyttelsesrådet beslutte, om rådet vil afgive udtalelse. Udtalelsen skal vedtages indenfor en måned. For Kommissionen gælder efter artikel 59 en frist på 10 uger til at vedtage en udtalelse i de sager, som er rejst. I denne periode må de nationale tilsyn ikke træffe afgørelse i sagen.

Også henset til, at anvendelsesområdet for artikel 58, stk. 2, litra a, forekommer bredt, ser Advokatrådet med betydelig skepsis på et system, hvor et europæisk databeskyttelsesråd skal have de nationale tilsynsmyndigheders afgørelser forelagt, f.eks. indenfor området af elektroniske serviceydelser, og at Kommissionen i medfør af artikel 60 tillægges kompetence til at suspendere et nationalt tilsyns afgørelse.

Systemet forekommer unødigt ressourcekrævende og til skade for nærhedsprincippet, ligesom det heller ikke synes at være realistisk, at sådanne sager kan håndteres og koordineres på en tilfredsstillende og retssikkerhedsmæssig forsvarlig måde indenfor de givne frister. Endelig frygter Advokatrådet, at systemet, som det er beskrevet, generelt vil medføre længerevarende sagsbehandlingstider for borgere og virksomheder og dermed hæmme udviklingen.

Advokatrådet finder derfor, at der skal arbejdes for, at afgørelseskompetencen i videst muligt omfang ligger hos de nationale datatilsyn. Som nævnt vurderer Advokatrådet, at vejledende udtalelser og guidelines vil give et mere fleksibelt, mindre ressourcekrævende og mere naturligt udviklingsforløb inden for persondataretten.

2.17 Det Europæiske Databeskyttelsesråd

Databeskyttelsesrådet består af de uafhængige datatilsyn, men også af en repræsentant fra Kommissionen, som ikke kan anses for uafhængig. Databeskyttelsesrådets formand skal omgående underrette Kommissionen om alle aktiviteter i databeskyttelsesrådet, og Kommissionen får ret til at anmode Databeskyttelsesrådet om at udføre opgaver og kan sætte frister for, hvornår Databeskyttelsesrådet skal yde rådgivning efter anmodning fra Kommissionen, jf. artikel 66.

Advokatrådet skal opfordre til, at Kommissionens rolle nøje vurderes, idet det efter Advokatrådets opfattelse alene bør være de uafhængige tilsyn, der forestår sammenhængsmekanismerne.

Endelig mener Advokatrådet, at der er behov for at vurdere Databeskyttelsesrådets kompetencer dels i forhold til de nationale tilsyns kompetencer, dels i forhold til indbringelse af Datatilsynets afgørelser for domstolene, jf. grundlovens § 63.

2.18 Anlæg af retssager mod andre lande tilsynsmyndigheder
Efter forordningsudkastets artikel 74, stk. 4, kan en registreret person anmode tilsynsmyndigheden i sin opholdsstat om at lægge sag an mod en anden tilsynsmyndighed, der har truffet en afgørelse, hvis vedkommende berøres af en sådan afgørelse fra en tilsynsmyndighed i en anden medlemsstat, der i første omgang har truffet afgørelsen. Bestemmelsen styrker borgernes retsstilling, men vil kræve betydelige ressourcetilførsel til Datatilsynet.

2.19 Bøder
Hvad angår forslagets administrative sanktioner skal Advokatrådet indstille, at det nøje overvejes, om det foreslåede niveau er i overensstemmelse med proportionalitetsprincippet. Det bemærkes, at område ikke synes fuldt ud sammenligneligt med konkurrenceretsområdet.

2.20 Anmeldelse
Advokatrådet hilser det velkomment, at forordningsudkastet afskaffer den hidtil kendte anmeldelsespligt, og skal samtidig opfordre til, at de bestemmelser i forslaget, der indfører en pligt til forudgående godkendelse fra eller forudgående høring af tilsynsmyndigheden, herunder visse overførsler til tredjelande, overvejes nøje, idet reglerne er administrativt byrdefulde for både virksomheder og myndigheder.

2.21 Insolvensområdet
Inden for insolvensområdet vil det være nødvendigt - eventuelt under domstolskontrol - at sikre, at kuratorer kan få adgang til de elektronisk lagrede oplysninger uden at skulle indhente samtykke. Advokatrådet skal opfordre til at der tages højde herfor i forslaget.

2.22 Udstedelse af delegerede retsakter
Som nævnt ser Advokatrådet med skepsis på, at Kommissionen - som ikke kan sidestilles med en uafhængig databeskyttelsesmyndighed - tillægges vidtgående kompetencer indenfor områder, der må anses for væsentlige.

Der er tale om områder, hvor der ofte fastsættes retningslinjer nationalt, enten i form af bestemmelser i særlovgivning, der præciserer i forhold til persondatalovens overordnede regler, eller som led i Datatilsynets praksis.

Databeskyttelsesområdet adskiller sig på grund af de uafhængige tilsynsmyndigheders nuværende rolle ganske markant fra andre områder, hvor der er tillagt Kommissionen

centrale kompetencer. Hertil kommer at der ikke er fastsat nogen tidshorisont, hvilket vil medfører en risiko for en betydelig grad af retsusikkerhed. Advokatrådet skal derfor opfordre til, at ethvert af de områder, hvor kompetencen delegeres til kommissionen nøje gennemgås, til afklaring af om det skønnes hensigtsmæssigt.

Det fremhæves i den forbindelse, at delegerede retsakter i traktatens TEUF's artikel 290 er beskrevet som ikke-lovgivningsmæssige retsakter, der udbygger eller ændrer visse ikke-væsentlige elementer i den lovgivningsmæssige retsakt.

3. Forholdet mellem forordningen og gældende regler

Justitsministeriet anfører i grundnotatet, at forordningsforslaget berører forhold, der har relevans for en række retsområder. Advokatrådet bakker op om, at det nøje vurderes hvilke danske love der skal ændres eller ophæves.

Med venlig hilsen

Torben Jensen

DANSKE
ADVOKATER

Justitsministeriet
Slotsholmsgade 10
1216 København K

jm@jm.dk

H.C. Andersens Boulevard 45
1553 København V

Telefon 33 43 70 00
mail@danskeadvokater.dk
www.danskeadvokater.dk

Dok.nr. D-2012-022248

6. juli 2012

Vedr.: Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

1. Indledning

Justitsministeriet har den 11. maj 2012 (j.nr. 2012-3756-0005) sendt forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) med anmodning om eventuelle bemærkninger senest den 1. juli 2012.

Forordningsforslaget har bl.a. til formål at ophæve og erstatte det gældende databeskyttelsesdirektiv med den konsekvens bl.a., at den regulering, der følger af persondataloven og anden lovgivning om behandling af personoplysninger, efter omstændighederne vil skulle ophæves eller ændres i overensstemmelse med den endelige forordning.

Forslaget vil medføre både administrative lettelser og administrative byrder for danske virksomheder.

Nedenfor under pkt. 2 er der redegjort for Danske Advokaters bemærkninger af mere generel og overordnet karakter. I forlængelse heraf indeholder pkt. 3 nogle bemærkninger til udvalgte dele af forordningsforslaget.

2. Generelle bemærkninger

Indledningsvis bemærkes det, at der kan rejses spørgsmål om det hensigtsmæssige i selve valget af en forordning som instrument på dette område fremfor et direktiv.

Som det fremgår af Justitsministeriets grund- og nærhedsnotat af 8. maj 2012, vurderes Kommissionens forslag at medføre såvel administrative lettelser som administrative byrder for danske virksomheder.

De administrative lettelser skyldes især hamoniseringen af databeskyttelseskrav og bestemmelsen om, at det alene er databeskyttelsesmyndigheden i det land, hvor selskabet har sit hovedkontor, der skal afgøre, om selskabet handler lovligt. Lettelserne vil derfor især vedrøre virksomheder, der opererer i flere EU-lande.

Forslaget vil imidlertid som anført også medføre en række byrder for erhvervslivet bl.a. som følge af bestemmelserne om dokumentation af databehandling og kravet om konsekvensanalyser vedrørende databeskyttelse, inden der foretages risikobehæftede databehandlinger.

Det fremgår af grund- og nærhedsnotatet, at de forventede administrative konsekvenser ved forslaget vil blive undersøgt nærmere med henblik på dels at kvantificere konsekvenserne for danske virksomheder, dels at komme med anbefalinger til, hvordan de administrative byrder i forslaget kan reduceres. Endvidere er det anført, at man fra dansk side vil arbejde for, at omkostningerne ved forslaget reduceres i forhold til Kommissionen forslag.

Der er både på EU – og nationalt plan i disse år stor fokus på erhvervsvirksomhedernes rammevilkår og på at bekæmpe administrative byrder for erhvervslivet.

Danske Advokater bemærker, at man er enig i behovet for, at der også i forhold til dette forordningsforslag bør være fokus på at finde den rette balance mellem på den ene side hensynet til databeskyttelse og på den anden side hensynet til virksomhedernes rammevilkår og de omkostninger, der er forbundet hermed. I den forbindelse bemærkes, at de administrative lettelser, der er lagt op til, nok snarere vil have betydning for store selskaber fremfor de små- og mellemstore virksomheder, der alene er til stede her i landet.

Danske Advokater deltager gerne i en eventuel nærmere udredning heraf.

Endvidere bemærkes det, at forordningsforslaget indeholder en række programerklæringer og nye begreber, ligesom der med forslaget er lagt op til et meget betydeligt antal delegerede retsakter, som selvsagt kan bringe i hvert fald nogen klarhed, men som samtidig gør det vanskeligt at forudse, hvordan det nærmere kommer til at virke i praksis. Hertil kommer, at der ikke er fastsat nogen tidshorisont. Dette indebærer, at der må forventes en ikke nærmere afgrænset periode med risiko for en ganske betydelig retsusikkerhed, som ikke mindst i lyset af de foreslåede bødeniveauer, jf. nedenfor, må være betænkelig.

I tilknytning hertil bemærker Danske Advokater, at det gældende regelsæt kan være vanskeligt at forstå og håndtere i praksis, og at der allerede i dag i forhold til persondataloven er visse fortolkningsspørgsmål og –tvivl, som forordningsforslaget ikke gør op med. Det gælder bl.a. med hensyn til afgrænsningen af henholdsvis dataansvarlig og databehandler.

Herudover bemærkes, at det forekommer vidtgående at tillægge Kommissionen kompetence til at udfylde interesseafvejningsreglen, jf. artikel 6, stk. 1, lit. f. Det samme gælder en eventuel afskaffelse af interesseafvejningsreglen som hjemmelsgrundlag inden for den offentlige forvaltning. Denne regel bidrager i dag i praksis til at gøre området operationelt.

Særligt med hensyn til tilsynet bemærker Danske Advokater, at der med det foreslåede nye retsgrundlag i endnu højere grad vil være behov for et smidigt tilsyn. Et sådant smidigt og effektivt tilsyn forekommer bedst at kunne sikres ved et nationalt tilsyn kombineret med den nuværende artikel 29-gruppe, der løbende afgiver vejledende udtalelser, der gælder for hele EU.

3. Bemærkninger til enkelte dele af forordningsforslaget

3.1. Det ansættelsesretlige område mv.

I forordningsforslaget er der lagt op til en række bestemmelser om behandling af personoplysninger, der har betydning i relation til ansættelsesforhold mv.

Det følger af bestemmelsen i persondataloven § 1, stk. 1, at loven gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Denne bestemmelse er suppleret af persondataloven § 1, stk. 2. Efter denne bestemmelse gælder loven for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold eller i øvrigt oplysninger om personlige forhold, som med rimelighed kan forlanges unddraget offentligheden.

Bestemmelsen i persondataloven § 1, stk. 2 følger ikke af direktivet (95/46/EF), og der er således tale om en særegen dansk regel. Bestemmelsen indebærer, at f.eks. fysiske samlinger af personalemapper, ansøgninger fra jobansøgere og mødereferater med oplysninger om identificerbare medarbejdere falder inden for lovens område. Dette ville ikke være tilfældet uden stk. 2, da sådanne samlinger ikke eller i hvert fald ikke altid antages at udgøre et "register" efter stk. 1.

Forslaget til forordning angiver samme materielle anvendelsesområde som persondatadirektivet og indeholder således ikke en regel svarende til persondataloven § 1, stk. 2. Forslaget indebærer derfor umiddelbart en forringelse af persondatabeskyttelsen, idet beskyttelsen ikke længere vil omfatte eksempelvis en samling af personalemapper. Det kan dog ikke afvises, at "register" vil blive fortolket bredere af EU-Domstolen til at omfatte f.eks. personalemapper.

Det bør - f.eks. i forordningens indledende betragtninger (præamblen) – afklares, om et "register" også omfatter en fysisk samling af personalemapper og lignende.

Efter gældende ret er samtykke kun gyldigt som behandlingsgrundlag, hvis der er tale om et reelt frivilligt samtykke. Der kan således være situationer, hvor den registrerede er under et så stort pres fra den dataansvarlige, at der ikke kan siges at foreligge et reelt frivilligt samtykke. Det er dog i dansk ret antaget, at den

omstændighed, at der er tale om et ansættelsesforhold - og således et vist afhængighedsforhold - ikke i sig selv indebærer, at et samtykke er ufrivilligt. Det er endvidere antaget, at den omstændighed, at en person giver et samtykke for at opnå en eller anden modydelse, f.eks. et job eller undgå at blive afskediget, ikke betyder, at samtykket er ufrivilligt.

I forordningsforslaget, jf. artikel 7, er der lagt op til, at samtykke ikke kan anvendes som behandlingsgrundlag i ansættelsesforhold. Af betragtning 34 fremgår således følgende:

> "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context."

Der er angiveligt tale om at ophæve arbejdsgiverens adgang til at benytte samtykke som databehandlingsgrundlag. Dette vil formentlig indebære en væsentlig administrativ byrde for arbejdsgiveren, idet arbejdsgiveren ved hver behandling af almindelige persondata vil skulle foretage en konkret vurdering af, om behandlingen falder ind under et af de andre (mere afvejningsbetingede) databehandlingsgrundlag.

I forhold til behandling af følsomme persondata er det ikke ualmindeligt, at medarbejderen af egen drift oplyser arbejdsgiveren om f.eks. helbredsmæssige forhold i forbindelse med sygdom. Efter gældende ret vil behandlingsgrundlaget for denne indsamling være samtykke, idet medarbejderen ved selv at have afgivet oplysningerne i sagens natur har samtykket til arbejdsgiverens viden om de helbredsmæssige forhold.

Efter forordningen vil arbejdsgiveren dog ikke kunne anvende samtykke som behandlingsgrundlag, og der vil næppe kunne findes andet anvendeligt behandlingsgrundlag for denne og lignende situationer. Arbejdsgiveren vil således have overtrådt forordningen, og selvom arbejdsgiveren - som følge af manglende forsæt/uagtsomhed - ikke kan pålægges bøde, forekommer dette ikke hensigtsmæssigt eller rimeligt. Der er tale om en ret indgribende ændring i retstilstanden for arbejdsgivere.

Formålet med forordningen er som anført ovenfor at totalharmonisere medlemsstaternes regulering af persondatabeskyttelse. Forordningsforslaget anerkender dog, at der på arbejdsmarkedet er særlige hensyn, der kan berettige visse nationale særregler. I forslagets artikel 82 op er der åbnet op for det.

Det fremgår af artikel 82, at medlemsstaterne kan fastsætte egne regler omkring en række forhold på arbejdsmarkedet, dog på den væsentlige betingelse, at der er tale om regler "[w]ithin the limits of this Regulation". Der synes således ikke at være mulighed for nationalt at fastsætte strengere regler end de, som fremgår af forordningen. Endvidere fremgår det af artikel 82(3), at Kommissionen kan fastsætte nærmere krav til medlemsstaternes udnyttelse af denne mulighed.

Det bør tydeliggøres, hvilke muligheder der præcis ligger i artikel 82(1) for at gennemføre nationale særregler, og dermed også hvad der nærmere forstås med "[w]ithin the limits of this Regulation."

Et meget væsentligt spørgsmål er desuden, i hvilket omfang forordningen tillader, at arbejdsmarkedets parter fortsat indgår kollektive aftaler om persondatabeskyttelse, idet der navnlig i samarbejdsudvalgssystemet behandles forhold omkring persondatabeskyttelse.

Artikel 82 vedrører efter sin ordlyd alene regler fastsat af medlemsstaterne ("Member States may adopt by law specific rules") og regulerer derfor ikke umiddelbart kollektive aftaler om persondatabeskyttelse. Forordningens totalharmoniserende formål taget i betragtning kan det dog ikke afvises, at det er Kommissionens hensigt, at det er det brede statsbegreb, der finder anvendelse, således at der ved "medlemsstat" forstås også faglige sammenslutninger, der fastsætter løn- og ansættelsesvilkår.

Det følger af artikel 152 TEUF, at:

> "Unionen anerkender og fremmer arbejdsmarkedsparternes rolle på EU-plan under hensyntagen til de nationale systemers forskelligartede karakter. Den letter dialogen mellem dem og respekterer deres uafhængighed."

Der er derfor traktatmæssig støtte – juridisk såvel som politisk – for, at der bør være adgang til kollektivt at aftale tilpasninger på området for persondatabeskyttelse.

3.2. Databeskyttelsesansvarlige

Det følger af forordningsudkastets artikel 35, at alle offentlige myndigheder og virksomheder med flere end 250 skal udpege databeskyttelsesansvarlige, som skal medvirke til at sikre, at forordningen overholdes.

Det fremgår af artikel 35(7), at den databeskyttelsesansvarlige nyder en væsentlig stillingsbeskyttelse:

> "During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties."

Da begrebet "dismissal" kan dække såvel afskedigelse som bortvisning, bør det præciseres, hvilke situationer der er omfattet. Det forekommer i den forbindelse ikke rimeligt, hvis en arbejdsgiver er forhindret i at bringe ansættelsesforholdet til ophør som følge af væsentlig misligholdelse (bortvisning).

Endvidere bør man søge at få klarhed omkring forholdet mellem de strafferetlige og civilretlige sanktioner for overtrædelse af bestemmelsen. Der bør således tages stilling til, om den pågældende kan kræve egentlig genansættelse, hvilket vil være atypisk i forhold til dansk ansættelsesret. Det kunne med fordel også i præamblen angives, om medlemsstaterne efter artikel 78 er forpligtede til at etablere et sanktionssystem i stil med det, der kendes fra området for ligebehandling og ikke-diskrimination. Ordlyden af artikel 78 kunne umiddelbart tyde på, at dette er tilfældet.

3.3. *Anmeldelse af brud på datasikkerheden*

Særligt med hensyn til den foreslåede bestemmelse i artikel 31, stk. 1, bemærkes det, at fokus i forhold til denne bestemmelse efter Danske Advokaters opfattelse bør være på, at virksomhederne iværksætter foranstaltninger for at hindre og stoppe eventuelle sikkerhedsbrist. Hertil kommer, at der bør foretages en nærmere vurdering i forhold til spørgsmålet om selvinkriminering. Det bemærkes også, at anmeldelse til tilsynet alene bør ske i tilfælde af mere alvorlige sikkerhedsbrist.

3.4. *Sanktioner*

Det fremgår af grund- og nærhedsnotatet, at regeringen finder, at forordningsforslagets administrative sanktioner, som i visse tilfælde indebærer et meget højt bødeniveau, må overvejes med henblik på at sikre, at de foreslåede administrative sanktionsniveauer er i overensstemmelse med proportionalitetsprincippet.

Danske Advokater er enig i, at der med forordningsforslaget er lagt op til et meget højt bødeniveau. I den forbindelse bemærkes det, at der må være betænkeligheder forbundet med en retstilstand, hvor der fastsættes meget betydelige bøder for overtrædelser af mere formel karakter, der ikke kan siges at have reel betydning for den enkelte person. Nærmere overvejelser herom bør ske i overensstemmelse med proportionalitetsprincippet.

3.5. *Det insolvensretlige område*

Danske Advokater bemærker, at der i det videre arbejde er behov for at sikre, at kuratorer kan få adgang til elektronisk lagrede oplysninger, uden at der skal indhentes samtykke. Det er nødvendigt for, at kurator kan udføre det arbejde, der følger af konkurslovens regler.

Det sene svar beklages.

Med venlig hilsen

Paul Mollerup
Adm. direktør

Fra: Scharf, Line [LSC@ankl.dk]
Sendt: 30. maj 2012 15:58
Til: Justitsministeriet
Emne: j.nr. 2012-3756-0005 - høringssvar

Under henvisning til Justitsministeriets brev af 11. maj 2012 skal jeg udtale, at forordningen om beskyttelse af fysiske personer i.f.m. behandling af personoplysninger mv. ikke giver Foreningen af Offentlige Anklagere anledning til bemærkninger, ud over det der allerede fremgår af grundnotatets punkt 8.

Med venlig hilsen

Line Scharf
bestyrelsesmedlem
-

Statsadvokaten for Midt-, Vest- og Sydsjælland, Lolland og Falster
Jens Kofods Gade 1, 3. tv.
1268 København K
Telefon 33 30 73 56 (direkte)

May 2012

MasterCard Comments – General Data Protection Regulation

Presentation of MasterCard

MasterCard is a global payments and technology company with its European headquarters in Waterloo, Belgium. It operates a four-party payment network, that links Issuers (i.e. the financial institutions issuing payment cards bearing the MasterCard brand) and Acquirers (i.e. the financial institutions that enter into contracts with merchants to accept MasterCard-branded payment cards) around the globe to facilitate the processing of card transactions.

MasterCard's primary customers are the issuing and acquiring financial institutions which have the direct contractual and financial relationship with the cardholders and merchants respectively. MasterCard itself is not a financial institution. It owns the MasterCard family of brands (including MasterCard, Maestro and Cirrus) and licenses financial institutions to use those brands in conducting card issuing and acquiring functions. MasterCard also provides the networks through which those these financial institutions interact to complete MasterCard-branded payment transactions, and sets certain rules, including rules governing fraud prevention and security requirements, regarding those interactions.

When processing a payment card transaction, the only personal data that MasterCard typically processes are card account numbers and related transaction details, except where additional personal data (e.g. name, address) are voluntarily provided by data subjects in such contexts as marketing activities that MasterCard may from time to time engage in with its cardholders and its merchants (e.g., MasterCard-controlled rewards programs, contests and promotions, etc.).

MasterCard's comments

Please find below MasterCard's 11 main concerns on the proposed General Data Protection Regulation ("Regulation") adopted by the Commission on January 25, 2012:

- MasterCard fully supports the choice of a **Regulation** over a Directive, so as to ensure full harmonization of the data protection rules in Europe, but regrets that it does not integrate at least some of the provisions of the e-Privacy Directive.

- The proposal for a **Single Supervisory Authority** providing a "one-stop-shop" is also a major improvement to the benefit of both EU companies and citizens, but it should be clarified that joint controllers – whether belonging to the same group of enterprises or not – are entitled to designate one competent authority for a given activity.

- The Regulation should clarify the concepts of **personal data** – in particular the "reasonably likely test" – and **data controllers** – by focusing on the determination of the purposes (irrespective of the means and conditions) as the only criteria to qualify a data controller;

- The Regulation should incentivize **anonymization and pseudonymization** of data, with a view to strengthen the protection of consumers' human rights and boost consumers' trust in the digital economy while enabling business and trade in the Union.

- The Regulation should require that the legal arrangements to be entered into by **joint controllers (Art. 24)** reflect the reality of their relationship (i.e. effective roles and direct/indirect relationship with the data subject) and determine their respective liabilities towards data subjects, so as to take the complexities of today's digital economy into account; otherwise, the risk of absolute joint liability is likely to deter economic operators from doing business in the Union, to the detriment of the growth of the whole European economy.

- The definition and regime of **profiling** (Art. 20) should be revisited so as to exempt or facilitate data processing for the purpose of fraud monitoring and prevention as well as online security, which are essential to build consumers' trust in the digital economy.

- The proposal to abolish the prior notification regime is very much welcome but has unfortunately be replaced by even more **bureaucracy** and burdensome requirements; in particular, Privacy Impact Assessments should only be conducted for a *clear and limitative* list of processing activities presenting specific risks; absent such changes, EU businesses would be put at a serious competitive disadvantage in relation to their counterparts in other jurisdictions, ultimately resulting in the slowdown of economic activities in the Union.

- **The prior consultation obligation** undermines the accountability regime based on *ex post* oversight and should be abolished for companies having appointed a data protection officer; if the Regulation is adopted as such, it is to be feared that supervisory authorities will be inundated with consultation requests, leading to a serious backlog at regulators, thereby significantly delaying the launch of new and innovative products and ultimately hindering innovation and economic growth in the Union.

- While the **consistency mechanism** is to be promoted, its process and time-limits should be clarified and significantly shortened to an overall process of four (4) months maximum; if not, EU businesses will be in limbo, unable to move commerce and trade forward, resulting in serious harm to innovation and economic growth in the Union.

- The Regulation should expressly state whether (or not) **prior authorization** is required when transferring data to third country public authorities in the context of previously approved regulatory activities, for instance data requests justified on the grounds of national laws aimed at the prevention of Anti-Money Laundering and/or the fight against terrorist financing.

- A longer **phase-in period** should be provided for with respect to the application of the Regulation to processing activities existing on the date of its entry into force, at least for industries (such as the payment industry) characterized by a multitude of partners/clients involved in the data processing activities, to avoid causing havoc and economic life disruption across all Europe.

Fra: Kirsten Dybvad Mikkelsen [kmi@ruc.dk]
Sendt: 1. juni 2012 11:11
Til: Justitsministeriet
Cc: journalen@ruc.dk; Kenja Friis Henriksen
Emne: Høring over Europa-Kommissionens forslag til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, RUC J.nr. 2006-00-820-0001

Vedr. j.nr. 2012-3756-0005.

Justitsministeriets iværksatte høring jfr. nedenfor giver ikke Roskilde Universitet anledning til bemærkninger.

Venlig hilsen

Kirsten Dybvad Mikkelsen
Juridisk chefkonsulent, Cand.jur.
Telefon: 4674 3159
Mobil: 2935 5547

Rektorsekretariatet, RUC
www.ruc.dk/om-universitetet/organisation/administration/

Følg RUC på ☐ FaceBook ☐ Twitter ☐ YouTube

Roskilde Universitet uddanner bachelorer, kandidater og ph.d.'er, der er rustet til at udfordre det fremtidige samfunds behov for nytænkning og problemløsning.

Fra: Justitsministeriet [mailto:jm@jm.dk]
Sendt: 11. maj 2012 14:18
Til: aau@aau.dk; au@au.dk; samfund@advokatsamfundet.dk; samfund@advokatsamfundet.dk; ac@ac.dk; amnesty@amnesty.dk; ae@ae.dk; ams@ams.dk; at@at.dk; bat@batkartellet.dk; ¤ Beskæftigelsesmin.; bl@bl.dk; bfid@scanpharm.dk; spt@spt.dk; kontakt@bryggeriforeningen.dk; brd@brd.dk; cbs@cbs.dk; apotekerforeningen@apotekerforeningen.dk; dpu@dpu.dk; info@shipowners.dk; drf@travelassoc.dk; dst@dst.dk; da@da.dk; info@danskbyggeri.dk; de@de.dk; export@dk-export.dk; info@danskerhverv.dk; di@di.dk; adm@nodeco.dk; metal@danskmetal.dk; frederikshavn@danskmetal.dk; drefo@drefo.dk; kontakt@akutmedicin.org; retsmedicinsk.institut@forensic.ku.dk; dansk.standard@ds.dk; dsr@dsr.dk; dts@dts.dk; varefakta@varefakta.dk; info@danskeark.dk; regioner@regioner.dk; post@dasp.dk; dt@datatilsynet.dk; sekretariat@patentagentforeningen.dk; region@region.dk; komite@rm.dk; dnvk@dnvk.dk; vek@rn.dk; hob@regionsjaelland.dk; komite@regionsyddanmark.dk; info@etiskraad.dk; fi@fi.dk; general@cochrane.dk; fi@fi.dk; itek@di.dk; digst@digst.dk; di@di.dk; $Direktoratet for Kriminalforsorgen; djoef@djoef.dk; dommerforeningen@gmail.com; hoeringer@dommerfm.dk; brostroem@privat.dk; post@domstolsstyrelsen.dk; drrb@drrb.dk; dsi@dsi.dk; evm@evm.dk; erst@erst.dk; 3f@3f.dk; fdb@fdb.dk; post@finansogleasing.dk; fm@fm.dk; mail@finansraadet.dk; finanstilsynet@ftnet.dk; forbrugerombudsmanden@fs.dk; fbr@fbr.dk; lars.thomsen.mikkelsen@get2net.dk; djoef@djoef.dk; info@bsa.org; lmc001@politi.dk; fri@frinet.dk; fsr@fsr.dk; info@advokatinkasso.dk; fp@forsikringogpension.dk; fmn@fmn.dk; ¤Frederiksberg Kommune; ftf@ftf.dk; info@ejendomsforeningen.dk; journal@ghsdk.dk; hk@hk.dk; sb@asb.dk; kake@domstol.dk; horesta@horesta.dk; hvr@hvr.dk; ida@ida.dk; center@humanrights.dk; itb@itb.dk;

Fra: Dot Bresdahl [DB@ac.dk]
Sendt: 18. juni 2012 09:27
Til: Justitsministeriet
Cc: 'jap@tdl.dk'
Emne: Vedr. Deres j.nr. 2012-3756-0005
Vedhæftede filer: Tandlægeforeningen - høringssvar - Behandling af personoplysninger.pdf

Til Justitsministeriet

AC fremsender hermed Tandlægeforeningens høringssvar vedr.
Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

Med venlig hilsen

Dot Bresdahl
Afdelingssekretær

D 2249 5860
E db@ac.dk

AKADEMIKERNES
CENTRALORGANISATION
T +45 3369 4040
F +45 3393 8540

E ac@ac.dk
W www.ac.dk

Tandlægeforeningen

Akademikernes Centralorganisation
Att. Afdelingssekretær Dot Bresdahl
Sendt via e-mail: db@ac.dk

Tandlægeforeningen
Amaliegade 17
1256 København K

Tel.: 70 25 77 11
Fax: 70 25 16 37
info@tandlaegeforeningen.dk
www.tandlaegeforeningen.dk

CVR nr. 21318418

Dato: 8. juni 2012

Sagsbeh.: KHS

Vedr.: Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

AC har ved e-mail af 14. maj i år udbedt sig Tandlægeforeningens eventuelle bemærkninger til det ovenfor nævnte forslag.

Tandlægeforeningen har nedenstående bemærkninger til det fremsendte:

Tandlægeforeningen kan konstatere, at Europa-Kommissionen med forordningsforslaget vil ophæve og erstatte det gældende databeskyttelsesdirektiv (direktiv 95/46/EF) og dermed også den danske persondatalov (lov nr. 429 af 31. maj 2000) samt andre love og bekendtgørelser, der vedrører behandling af personoplysninger.

Tandlægeforeningen mener, at det er godt, at EU´s borgere, mv. ved en forordning sikres ensartethed på området. Der er to væsentlige fordele ved dette:

- For det første har forordningen direkte virkning og dermed kan medlemsstaterne ikke indføre særregler på området, hvorved man fjerner det uhensigtsmæssige i, at medlemsstaterne har kunnet implementere 1995-direktivet forskelligt.
- For det andet sikres en ensartet fortolkning på tværs af landegrænserne i EU.

Forordningen vil ifølge Kommissionen medføre administrative lettelser og dermed besparelser for virksomheder og organisationer.

Tandlægeforeningen mener, at forslaget ligeledes vil medføre administrative byrder for danske virksomheder og dermed udgifter. Eksempelvis til personale, som skal være på forkant med, at virksomheden lever op til lovgivningen, især hvis det foreslåede bødeniveau bliver en realitet, se nedenfor. Virksomheder og organisationer med over 250 ansatte pålægges ligeledes at oprette en ekstra chefpost til en databeskyttelsesansvarlig.

I Danmark har bødestørrelserne på persondataområdet indtil videre været yderst overkommelige. Datatilsynet kan i dag uddele næser og i visse sager

foretage politianmeldelse. Bødeniveauet for overtrædelse af persondataloven ligger typisk på 5 - 10.000 kr.

Forslaget lægger op til, at bøderne fremover kan udgøre op til EUR 250.000 og 1. mio. alt efter karakteren af overtrædelsen. Alternativt, når der er tale om virksomheder, kan der alt efter karakteren af overtrædelsen opkræves op til 2 % af virksomhedens årlige globale omsætning for overtrædelse af persondatareglerne. Forslagets artikel 79 oplister en række overtrædelser, f.eks. manglende udpegning af en databeskyttelsesansvarlig.

Henset til, at udviklingen på området igennem de sidste 17 år har ændret sig markant er der ingen tvivl om, at der er behov for en videregående regulering af persondataretten og Tandlægeforeningen kan som udgangspunkt støtte det fremsendte forslag.

Tandlægeforeningen finder dog ikke, at nationale tilsynsmyndigheder bør kunne pålægge virksomheder og myndigheder bøder i de meget høje niveauer med fare for at proportionalitetsprincippet krænkes. Tandlægeforeningen foreslår derfor, at bødeniveauet nedsættes og at bøder over EUR 400.000 henlægges til domstolsafgørelse.

Med venlig hilsen

Freddie Sloth-Lisbjerg
Formand

Joakim Lilholt
Direktør

Justitsministeriet
Slotsholmsgade 10
1216 København K

14. juni 2012

J.nr. 0141-20120002-3

Høringssvar, j.nr. 2012-3756-0005

Ved mail af 11. maj 2012 har Justitsministeriet anmodet Patientforsikringen om eventuelle bemærkninger vedrørende Europa-Kommissionens forslag til Europa-Parlementets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) med høringsfrist den 1. juli 2012.

Patientforsikringens bemærkninger:

For så vidt angår artikel 33 om konsekvensanalyse vedrørende databeskyttelse, går vi ud fra, at Patientforsikringen er omfattet af undtagelsesbestemmelsen i artikel 33, nr. 5, sammenholdt med artikel 6, stk. 1, litra c, idet vi i netop denne sammenhæng må anses som et offentligt organ, og idet vi efter lov om klage- og erstatningsadgang inden for sundhedsvæsnet er forpligtet til at behandle patientskadesager.

Med venlig hilsen

Karen Inger Bast
direktør

Nytorv 5, 3. sal
1450 København K

Tel: 3312 4343
Fax: 3312 4341

pf@patientforsikringen.dk
www.patientforsikringen.dk

Patientforsikringen

Experian™
A world of insight

Justitsministeriet
Slotsholmsgade 10
1216 København K
Brevet er sendt elektronisk til: jm@jm.dk

København, den 28. juni 2012

HØRINGSSVAR – EU-KOMMISSIONENS FORSLAG NY DATABESKYTTELSESFORORDNING (DERES J.NR. 2012-3756-0005)

Vi henviser til Justitsministeriets høringsbrev af 11. maj 2012.

Experian er en global leverandør af kreditoplysningstjenester og har virksomhed i 15 lande i Europa, herunder Experian A/S i Danmark, som blandet andet drifter RKI registret over dårlige betalere. Experian støtter formålet med EU-kommissionens forslag til nye databeskyttelsesregler og arbejdet med at hæve det generelle niveau for databeskyttelse for enkeltpersoner og opnå konsistens på tværs af landegrænser. Experian er imidlertid bekymret for, at forslaget kan have alvorlige, negative konsekvenser for kreditoplysningsbureauerne. Experian tror imidlertid at disse mulige konsekvenser er utilsigtede.

De tjenester, der udbydes af kreditoplysningsbureauer, er bredt anerkendt som værende afgørende for at være i stand til at foretage en effektiv økonomisk styring i lande med et veludviklet økonomisk system. Såfremt udbuddet eller anvendelsen af disse tjenester afskæres eller indskrænkes vil dette have en skadelig effekt på adgangen til kredit for såvel privatpersoner som virksomheder. Dette vil hæmme den økonomiske vækst i Danmark. Det vil også være forbundet med alvorlige konsekvenser for forbrugerne, såfremt långivers adgang til anvendelse af kreditoplysninger afskæres eller indskrænkes. Kredit vil generelt blive sværere at opnå, fordi forbrugerne ikke på samme måde vil kunne bevise deres kreditværdighed, imens andre forbrugere vil blive bevilliget kredit, som de ikke kan tilbagebetale. Som konsekvens vil låntagernes beslutningstagning når der anmodes om kredit blive mindre objektiv og dermed mindre retfærdig.

Om sammenhængen mellem de særlige danske regler om kreditoplysningsvirksomhed i lov om behandling af personoplysninger ("Persondataloven") kap. 6 og persondatadirektivet 95/46/EF ("Direktivet") bemærkes, at de danske regler i Persondataloven om kreditoplysningsvirksomhed i det væsentlige svarer til de regler, som var indeholdt i lov om private registre kap. 3, der var gældende inden Persondatalovens ikrafttræden. Reglerne har således ikke et direkte modstykke i Direktivet, men Justitsministeriet har vurderet, at reglerne i kap. 6 falder inden for de rammer, som Direktivet giver for at fastsætte særlige regler om behandling af personoplysninger på nærmere bestemte områder. Reglerne i Persondatalovens kap. 6 gælder ikke alene for behandling af kreditoplysninger om fysiske personer, men også for behandling af kreditoplysninger om juridiske personer. Idet omfang spørgsmål om kreditoplysningsbureauers virksomhed ikke er reguleret i Persondatalovens kap. 6., gælder Persondatalovens almindelige regler.

Experian ønsker i dette høringssvar at redegøre for de negative konsekvenser, forslaget kan have for kreditoplysningsbureauer. Videre vil Experian give eksempler på, at mange af de af EU-kommissionen foreslåede databeskyttelsesregler og - principper allerede eksisterer i dansk ret.

Den foreslåede regulering i form af en forordning (i stedet for dagens direktiv), vil formentlig indebære at flere af de eksisterende danske databeskyttelsesregler ikke kan opretholdes. Experian mener, at Danmark i de kommende forhandlinger bør arbejde for status quo (dvs. opretholde de nuværende regler) på følgende punkter: (1) profilering , (2) data minimering , (3) vilkåret om berettiget interesse, og (4) den registreredes rettigheder. Disse punkter vil blive gennemgået i det følgende.

1. RESTRIKTIONER VEDRØRENDE FORANSTALTNINGER BASERET PÅ PROFILERING (ARTIKEL 20)

Suggested Amendment

Article 20

Measures based on profiling

1. Every natural person shall have the right to request not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: ...

(c) is consistent with the requirements of Article 6 and of this Article 20 ~~based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards~~.

Add wording into Article 20 to allow the following:

A requirement on data controllers to notify the data subject where such processing takes place, and giving the individual the right to have any such decision reviewed.

Experian mener at den foreslåede artikel 20 – restriktioner vedrørende foranstaltninger baseret på personprofilering - efter sin ordlyd må antages at kunne hindre fortsat anvendelse af de scoringsmodeller, der i dag i vidt omfang benyttes i kreditoplysningsvirksomhed. Forskellige typer scoringsmodeller er af væsentlig betydning for Experians virksomhed og er anerkendt som en effektiv, transparent, pålidelig og ikke-diskriminerende måde at behandle store mængder data til brug for kreditvurderinger.

Experian er desuden af den opfattelse, at de personprofiler der anvendes i forbindelse med kreditoplysningsvirksomhed klart skiller sig fra de personprofiler der anvendes i tilknytning til sociale medier.

I henhold til Datatilsynets praksis (j.nr. 2005-631-0161) er et kreditoplysningsbureau ikke berettiget til at videregive kreditoplysninger om enkeltpersoner i form af en score, der alene beregnes på grundlag af oplysninger om seneste adresseændring, postnummer og fødselsår, uden at inddrage oplysninger om den konkrete persons økonomiske forhold, f.eks. misligholdte fordringer. Baggrunden er, at hvis

kreditoplysningsbureauet ikke inddrager økonomiske oplysninger, vil en sådan score ikke i alle tilfælde være en oplysning af betydning for bedømmelsen af den pågældende persons økonomiske soliditet, hvilket er en forudsætning for at behandle oplysningen i medfør af Persondatalovens § 20.

Det fremgår desuden af afgørelsen, at det er afgørende for, om en oplysning må behandles af et kreditoplysningsbureau, om oplysningen har betydning for vurderingen af den registreredes betalingsevne i andre fremtidige skyldforhold.

Der findes således allerede i dag i dansk ret restriktioner på foranstaltninger baseret på profilering. Experian mener derfor ikke, at den foreslåede artikel 20 er nødvendig– og at den til dels er uheldig, da den må antages at ville ramme de scoringsmodeller, der benyttes i kreditoplysningsvirksomhed – og at de nuværende regler på området derfor bør opretholdes.

2. DATAMINIMERING (ARTIKEL 5)

Suggested Amendments

Article 5

Principles relating to personal data processing

Personal data must be: ...

(c) adequate, relevant, and proportionate~~limited to the minimum necessary~~ in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

(d) accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay;

Experian er af den opfattelse, at den foreslåede artikel 5 om adgangen til at opbevare og behandle store mængder information, vil medføre en begrænsning for kreditoplysningsbureauerne.

Kreditoplysningsvirksomhed forudsætter opbevaring af data i en længere tidsperiode bl.a. med henvisning til den registreredes tidligere adresser og/eller identiteter. Den måde kreditoplysningsbureauerne i dag er opbygget på sikrer imidlertid, at unødvendig opbevaring af data og opbevaring af data i længere tid end nødvendigt undgås.

De danske regler for behandling af oplysninger i forbindelse med kreditoplysningsvirksomhed fremgår dels af Persondatalovens § 20 og dels af Datatilsynets standardvilkår for kreditoplysningsbureauer.

Det følger af Persondatalovens § 20, at kreditoplysningsbureauer kun må behandle oplysninger, som er af betydning for bedømmelsen af økonomisk soliditet og kreditværdighed, og der må ikke behandles

oplysninger om personers rent private forhold. Der må endvidere ikke behandles oplysninger, som er mere end fem år gamle, medmindre der er tale om objektive oplysninger, som f.eks. identifikationsoplysninger, eller oplysninger, der er positive for den pågældende. I en række tilfælde gælder der væsentligt kortere slettefrister, bl.a. i forhold til arrest, betalingsstandsning og gældssanering.

Det følger endvidere af Datatilsynets standardvilkår for kreditoplysningsbureauer, at det påhviler kreditoplysningsbureauet at godtgøre registreringens berettigelse, når der af en registreret rejses tvivl om dennes rigtighed, jf. pkt. 5. Der må endvidere ikke behandles oplysninger om fordringer, der bestrides, førend tvisten er endeligt afgjort ved domstolene.

Det er vanskeligt at vurdere, om den foreslåede formulering vil medføre en skærpelse af de gældende danske regler, men der er ikke i de nugældende regler formuleret et absolut princip om dataminimering. Experian mener, at idet der allerede i dag findes særlige regler om registrering og behandling af oplysninger til brug for kreditvurdering i dansk ret, som giver den nødvendige og tilstrækkelige beskyttelse for de registrerede og samtidig anerkender behovet for at registrere og behandle information i en længere periode til brug for kreditvurdering, bør dagens regler opretholdes.

3. LOVLIG BEHANDLING AF PERSONOPLYSNINGER (ARTIKEL 6)

Suggested Amendments

Article 6

Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(f) processing is necessary for the purposes of the legitimate interests pursued by thea controller or by the third party or third parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Experian mener, at den foreslåede formulering af Forordningens artikel 6, stk. 1, litra f), er en skærpelse i forhold til de gældende regler i Direktivets artikel 7, litra f), fordi der ikke er en udtrykkelig henvisning til at behandling af personoplysninger kan ske af hensyn til en tredjemands interesser.

De danske regler om videregivelse af kreditoplysninger fremgår af Persondatalovens § 23. Bestemmelsen beskriver ikke på samme måde som Direktivet og den foreslåede Forordning interesseafvejningen, men det må anses for forudsat med reglerne, at der kan ske behandling af hensyn til kreditoplysningsbureauernes abonnenter (tredjemand). Det er således forudsat i dansk ret, at der kan ske en behandling på vegne af tredjemands interesser.

Det er Experians opfattelse, at den foreslåede formulering af Forordningens artikel 6, stk. 1, litra f) formentlig er ment som en videreførelse af Direktivets artikel 7, litra f), men det er imidlertid ikke muligt for Experian at fastslå med sikkerhed om artikel 6, stk. 1, litra f) forudsætter en reel ændring sammenlignet med Direktivets artikel 7, litra f), og om den foreslåede formulering således vil indebære en skærpelse.

Experian vil gerne understrege den fortolkningstvivl som kan opstå såfremt den foreslåede artikel 6, nr. 1, litra f) implementeres i dansk ret. Experian mener at dagens retstilstand, hvorefter det er muligt at behandle data som følge af tredjemands interesser, bør opretholdes, fordi det er af stor betydning for blandt andet kreditoplysningsbureauerne at interesseafvejningen også inkluderer behandling af persondata indhentet af hensyn til tredjemands interesser.

4. DEN REGISTREREDEES RETTIGHEDER VED BEHANDLING AF KREDITINFORMATION

Suggested Amendments

A new article is included in "Chapter IX - Provisions relating to specific data processing situations":

Processing of credit files by credit reference agencies

1. Member States shall provide for exemptions or derogations from Articles 7, 12, 15, 16, 17 and 18, in order to reconcile the right to the protection of personal data with the rules governing *[the processing of personal data within credit files held by credit reference agencies]*. Such exemptions and derogations shall take into account the legitimate need for organisations active in the credit referencing and financial sectors and organisations providing supporting services in this respect to assess the economic situation and behaviour of data subjects based on all relevant available information in a continuous manner, as well as the right for data subjects to obtain clear, understandable information regarding their personal data and economic profile being maintained and processed by these organisations and organisations providing supporting services in this respect.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent law or amendment affecting them.

Experian foreslår, at der indsættes en ny artikel med hjemmel til, at medlemsstaterne kan fastsætte undtagelser og fravigelser i forhold til de registreredes rettigheder for så vidt angår kreditoplysningsvirksomhed.

Vi gennemgår nedenfor de nuværende danske regler vedrørende disse rettigheder.

4.1 Samtykke

I enkelte lande er behandling af kreditoplysninger baseret på samtykke fra den registrerede. De foreslåede stramninger vedrørende indhentelsen af samtykke vil begrænse adgangen til at basere behandlingen på et samtykke, jf. forslagets artikel 7.

De danske regler om behandling af kreditoplysninger bruger ikke samtykke som behandlingshjemmel. Det må antages, at behandling af kreditoplysninger baseret på samtykke fra den registrerede reelt vil gøre det umuligt for kreditoplysningsbureauerne at indsamle og behandle oplysninger, idet det må forventes, at meget få personer vil give deres samtykke til at der indsamles og behandles oplysninger om dem, når personerne ved, at dette vil påvirke deres kreditværdighed i negativ retning.

De danske regler forudsætter således som udgangspunkt, at behandlingen af kreditoplysninger ikke sker på grundlag af samtykke.

Der kan imidlertid tænkes formålstjenstligt at kunne foretage behandling af personoplysninger om rent private forhold om bl.a. pension, kontanthjælp eller lignende, hvis oplysningerne er indhentet på baggrund af den registreredes samtykke.

Baseret på det ovennævnte mener Experian derfor, at der er behov for undtagelse fra samtykkekravet for så vidt angår kreditoplysningsbureauernes behandling af kreditoplysninger.

4.2 Indsigtsret

Der er i flere jurisdiktioner, herunder i Danmark, fastsat specifikke regler om indsigtsret i kreditoplysninger. Experian mener, at de registrerede herved tilgodeses og sikres en hurtig og effektiv besvarelse af deres indsigtsanmodninger. Den foreslåede bestemmelse, jf. artikel 15, kan indebære at der fremadrettet vil ske meddelelse af mindre præcise og relevante oplysninger til de registrerede.

De danske regler fremgår af Persondatalovens § 22. I medfør af denne bestemmelse skal kreditoplysningsbureauer til enhver tid på begæring af den registrerede inden fire uger på en let forståelig måde meddele denne indholdet af de oplysninger og bedømmelser, som bureauet har videregivet om den pågældende inden for de sidste seks måneder, samt af de øvrige oplysninger, som bureauet opbevarer om den pågældende, herunder foreliggende bedømmelser.

Bureauet skal endvidere give oplysning om kategorien af modtagere af oplysningerne samt tilgængelig information om, hvorfra oplysningerne stammer. Den registrerede kan forlange, at bureauet giver en skriftlig meddelelse. Bureauet er berettiget til at kræve betaling for skriftlige meddelelser til den registrerede, jf. bekendtgørelse om betaling for skriftlige meddelelser fra kreditoplysningsbureauer.

Der er således i dansk ret i dag særlige regler for indsigtsret i kreditoplysninger.

4.3 Berigtigelse

Enkelte lande, herunder Danmark, har specifikke regler om berigtigelse af kreditoplysninger. Experian mener at den registrerede er bedst tjent med at disse regler, som sikrer den registrerede tilstrækkelige rettigheder, opretholdes.

I henhold til Persondatalovens § 24 skal oplysninger eller bedømmelser, der viser sig urigtige eller vildledende, snarest muligt slettes eller berigtiges.

Er en oplysning eller bedømmelse, der viser sig urigtig eller vildledende, forinden blevet videregivet, skal bureauet straks, i henhold til Persondatalovens § 25, give skriftlig underretning om berigtigelsen til den registrerede og til alle, der har modtaget oplysningen eller bedømmelsen inden for de sidste 6 måneder, før bureauet er blevet bekendt med forholdet. Den registrerede skal tillige have meddelelse om, hvem der har modtaget underretning efter 1. pkt., og hvorfra oplysningen eller bedømmelsen stammer.

Desuden foreskriver Persondatalovens § 26, at henvendelser fra en registreret om sletning, berigtigelse eller blokering af oplysninger eller bedømmelser, der angives at være urigtige eller vildledende, eller om sletning af oplysninger, der ikke må behandles, snarest og inden 4 uger efter modtagelsen skal besvares skriftligt af bureauet. Såfremt bureauet nægter at foretage en begæret sletning, berigtigelse eller blokering kan spørgsmålet indbringes for Datatilsynet. Bureauets svar til den registrerede skal indeholde information om adgangen til at indbringe spørgsmålet for Datatilsynet.

Der findes således allerede i dag i dansk ret specifikke regler for berigtigelse af kreditoplysninger. Experian er af den opfattelse, at disse regler giver den registrerede de nødvendige og tilstrækkelige rettigheder i forbindelse med sletning, berigtigelse og blokering af kreditoplysninger, og mener derfor, at disse regler også bør opretholdes fremadrettet.

4.4 Retten til at blive glemt

Experian mener, at retten til at glemt og til sletning, jf. artikel 17, ikke bør finde anvendelse uden modifikation i forhold til kreditinformationsvirksomhed. Baggrunden for dette synspunkt er, at de oplysninger som behandles af kreditoplysningsbureauerne har værdi for andre end den registrerede, og at udøvelse af denne ret reelt kan umuliggøre en korrekt vurdering af kreditværdighed.

Experian mener derfor, at der er behov for en undtagelse fra artikel 17 for så vidt angår oplysninger der benyttes af kreditoplysningsbureauerne til bedømmelse af økonomisk soliditet og kreditværdighed. Der er ikke i dag danske regler, der modsvarer den foreslåede ret til at blive glemt og til sletning.

4.5 Ret til dataportabilitet

Der er ikke i dag danske regler, der modsvarer den foreslåede ret til dataportabilitet og Experian mener ikke, at den foreslåede artikel 18 er egnet for så vidt angår de oplysninger, som opbevares og behandles af kreditoplysningsbureauerne.

I modsætning til data som uploades til sociale medier og data tilknyttet en persons forbrug af informationstjenester (for eksempel telefoni eller andre elektroniske hjælpemidler), ville det medføre en betydelig risiko at lade kreditoplysninger og relaterede data være underlagt retten til dataportabilitet. Dette skyldes blandt andet den specielt konfidentielle natur af disse data. Dataportabilitet ville potentielt indebære en betydelig øget risiko for svindeltilfælde (i tilfælde af overførsel til den forkerte person), øget sandsynlighed for brud på informationssikkerheden (hvis dataene blev overført af den registrerede til en upålidelig tredjemand), og for at kreditoplysninger bliver forfalsket eller manipuleret før videre overførsel.

Experian mener derfor, at der er behov for en undtagelse fra artikel 18 for så vidt angår kreditoplysningsvirksomhed.

Experian håber, at der vil blive taget hensyn til ovenstående kommentarer og synspunkter. Såfremt Justitsministeriet måtte have spørgsmål eller kommentarer, står vi selvfølgelig til Deres disposition.

Med venlig hilsen
Experian A/S

Heidi Hoelgaard
Head of Legal & Compliance, Nordic

DET KONGELIGE BIBLIOTEK

NATIONALBIBLIOTEK OG
KØBENHAVNS UNIVERSITETS-
BIBLIOTEK

POSTBOKS 2149
DK-1016 KØBENHAVN K

TEL: + 45 33 47 47 47
FAX: + 45 33 93 22 18
BANK: 0216 4069032583
CVR: 28 98 88 42
EAN: 5798 000 79 52 97
EMAIL: kb@kb.dk

Kulturministeriet
Att. fuldmægtig Helene Nordborg Kiær
hnk@kum.dk

J.nr. 2012-008246
Den 1. juni 2012

Høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse.

Kulturministeriet har anmodet Det Kongelige Bibliotek om bemærkninger til Europa-Kommissionens forslag til generel forordning om databeskyttelse.

Det Kongelige Bibliotek har modtaget Statsbibliotekets og Statens Arkivers høringssvar, hvori der redegøres for de bekymringer, som en vedtagelse af forordningen i dens nuværende form giver anledning til for biblioteker og arkiver. Det Kongelige Bibliotek tilslutter sig disse betragtninger.

Det Kongelige Bibliotek skal forvalte den nationale kulturarv, herunder håndskrifter, arkivalier, kort og den danske del af internettet i netarkivet. Biblioteket arbejder for at forenkle, effektivisere og udbygge adgangen til og benyttelsen af institutionens resurser, bl.a. via digitaliseringsinitiativer. Brugen af de digitale resurser vokser dramatisk og elektroniske downloads var i 2010 92 % af institutionens samlede udlån.

Som et eksempel på et nyt område, hvor biblioteket er nødt til at igangsætte et nyt digitaliseringsinitiativ til aflastning af den hidtidige fysiske indsamling, kan bibliotekets håndskriftsafdeling nævnes. Biblioteket har gennem mange år indsamlet forskellige kulturpersonligheders arkivalier, men i dag er brugen knyttet til e-mails og andre elektroniske medier, hvor det i gamle dage var breve, dagbøger og lignende. Biblioteket frygter, at dette initiativ kan umuliggøres, hvis forordningen gennemføres i den foreliggende form, jf. Statens Arkivers bemærkninger.

Det Kongelige Bibliotek finder således ikke, at der er en rimelig balance mellem hensynet til fysiske personers databeskyttelse og hensynet til informationsfriheden og bevaringen af og adgangen til kulturarven.

Venlig hilsen

Søren Clausen
Chefkonsulent

Morten Daniel Dahm-Hansen

Fra: Søren Riiskjær [soeren.riiskjaer@dgi.dk]
Sendt: 14. juni 2012 08:21
Til: Helene Nordborg Kiær
Cc: Steen F. Andersen DDS
Emne: SV: Høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse

Kære Helene

Tak for materialet – og for muligheden for at kommentere det.

DGI anerkender, at forslaget til forordning baserer sig på behovet for beskyttelse af personoplysninger, herunder Artikel 8 i EU Charter om grundlæggende rettigheder, og finder det positivt, at forslaget indeholder nye tiltag i form af retten til at blive glemt og skærpet beskyttelse imod at blive genstand for profilering. DGI finder det også positivt, at kravene til den registeransvarliges opbevaring af behandlingsdokumentation er begrænset i forhold til, hvilke virksomheder og organisationer, der er omfattet af kravet.

DGI, der varetager idrætsforeningernes interesser, har konstateret, at den gældende persondatalov (der bygger på det gældende databeskyttelsesdirektiv) på nogle punkter giver uhensigtsmæssigheder for foreningslivet. Specielt drejer det sig om interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7, der giver mulighed for behandling af oplysninger, hvis denne er nødvendig for at den dataansvarlig (foreningen) kan forfølge en berettiget interesse. Denne regel indebærer efter den af Datatilsynet fastlagte praksis nogle meget snævre grænser for, at en forening på sin hjemmeside kan offentliggøre medlemslister og eksempelvis holdbilleder. DGI ser gerne, at den nye forordning giver lempeligere rammer, når det drejer sig om harmløse oplysninger/billeder, selvom disse må anses for at være private oplysninger. Forslaget til forordning indeholder i Artikel 6, stk. 1, litra f en regel, der indebærer, at der kan behandles oplysninger, hvis behandlingen er nødvendig for at den registeransvarlige kan forfølge en legitim interesse. DGI ser derfor gerne belyst, hvorvidt forslaget til forordning vil give mulighed for en mere lempelig praksis på det anførte område.

Vi er usikre på, om forslaget berører etablering af et centralt register over dopingdømte, som det netop er foreslået af Kulturministeriets arbejdsgruppe vedr. motionsdoping – og i det hele taget den gældende praksis vedr. offentliggørelse af sanktioner på dopingområdet. Vi håber, Kulturministeriet vil være i stand til at belyse dette nærmere og imødegå utilsigtede og uhensigtsmæssige ændringer.

Venlig hilsen

Søren Riiskjær
Idrætspolitisk rådgiver

DGI
Direkte 79 40 40 95 | Mobil 20 23 66 61
Vingsted Skovvej 1 | 7100 Vejle
sb@dgi.dk | www.dgi.dk

DGI står også bag

Fra: Helene Nordborg Kiær [mailto:hnk@kum.dk]
Sendt: 25. maj 2012 10:09
Til: journalen@dr.dk; peso@dr.dk; Tv2@tv2.dk; liqv@tv2.dk; lh@antidoping.dk; pbr@dif.dk; Søren Riiskjær; jesper@firmaidraet.dk; MOB@danskerhverv.dk; ahe@sa.dk; Poul Olsen; scl@kb.dk; ekn@kb.dk; sb@statsbiblioteket.dk; hvh@statsbiblioteket.dk; Ministersager, Kulturstyrelsen
Cc: Bente Skovgaard Kristensen; Katrine Tarp; Camilla Vange Mynster; Tine Brøchner; Karen Søndergaard; Martin

STATSBIBLIOTEKET

VICTOR ALBECKS VEJ 1
8000 AARHUS C

8946 2022
sb@statsbiblioteket.dk
www.statsbiblioteket.dk

Danske Bank 02164069038514
CVR/SE 1010 0682
EAN 5798000791084

15. juni 2012
HvH

Kulturministeriet

Att: Fuldmægtig Helene Nordborg Kiær
hnk@kum.dk

Høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse

Statsbiblioteket takker for lejligheden til at kommentere Europa-Kommissionens forslag til generel forordning om databeskyttelse.

Statsbiblioteket har i sit høringssvar begrænset sig til forhold, der vedrører behandlingen af personoplysninger til historiske, statistiske eller videnskabelige forskningsformål.

Retten til at blive glemt

Et væsentligt formål med den nye forordning er, at styrke beskyttelsen af personoplysninger, herunder også at sikre personer "retten til at blive glemt". Dette formål rimer umiddelbart ikke godt med formålet for ABM institutioner, hvis fremmeste opgave er at bevare oplysninger, herunder også oplysninger, der kan henføres til identificerbare personer, med det formål, at de kan gøres til genstand for historisk eller videnskabelig forskning eller statistiske undersøgelser. Heldigvis fastslås det i Betragtning 53 at

" ... opbevaring af oplysningerne bør dog tillades, hvis det er nødvendigt til historiske, statistiske eller videnskabelige forskningsformål, af hensyn til samfundsinteresser på folkesundhedsområdet, med henblik på at udøve retten til ytringsfrihed, når det kræves i henhold til lovgivningen, eller hvis der er grund til at begrænse behandlingen af oplysninger i stedet for at slette dem."

Det vil sige, at der ikke skulle være noget til hinder for, at Statsbiblioteket fortsat kan bevare de dele af kulturarven, der også indeholder personoplysninger, til brug for historiske, statistiske eller videnskabelige forskningsformål, med henblik på at udøve retten til ytringsfrihed, og når det kræves i henhold til anden lovgivning, som f.eks. pligtafleveringsloven.

Forskning

Spørgsmålet er så, under hvilke betingelser denne forskning kan ske. Det fremgår af artikel 83.

Det fremgår af art. 83, stk. 1, at personoplysninger kun må behandles til historiske, statistiske eller videnskabelige forskningsformål, såfremt formålet ikke kan opfyldes ved brug af anonymiserede data, og at de oplysninger, der gør det muligt at knytte oplysninger til en identificeret eller identificerbar person, opbevares adskilt fra de øvrige oplysninger, *så længe disse formål kan opfyldes på denne måde* (min kursivering).

Vi opfatter tilføjelsen "*så længe disse formål kan opfyldes på denne måde*" således, at kravet om adskillelse af personoplysninger fra andre data kun gælder, såfremt det er muligt uden at forskertse forskningsformålet. I modsat fald vil Statsbiblioteket ikke kunne leve op til forordningens krav, f.eks. i henseende til forskning i Netarkivet eller radio og tv-arkivet, da det ikke er muligt at anonymisere data eller opbevare dem adskilt fra de øvrige oplysninger.

Offentliggørelse af forskningsresultater

Betingelserne for offentliggørelsen af forskningsresultater indeholdende personoplysninger, er beskrevet i art. 83, stk. 2,

Det bemærkes, at der tales om "Organer, der gennemfører historisk, statistisk eller videnskabelig forskning", hvilket efterlader spørgsmålet om, hvorledes enkeltpersoner, der gennemfører forskning er stillet. En meget stor del af den historiske og samfundsvidenskabelige forskning udføres af enkeltpersoner.

For at offentliggøre personoplysninger kræves, at den registrerede har givet sit samtykke til offentliggørelsen; at offentliggørelsen af personoplysninger er nødvendig for at fremlægge forskningsresultater eller fremme forskningen, *for så vidt den registreredes interesser, grundlæggende rettigheder eller frihedsrettigheder ikke tilsidesætter disse interesser* (min kursivering); eller at den registrerede selv har offentliggjort oplysningerne.

Vi forstå den kursiverede sætning sådan, at såfremt den registrerede ikke har givet samtykke eller selv har offentliggjort oplysningerne, så går den registreredes interesser forud for interessen i at fremlægge forskningsresultaterne eller fremme forskningen, og så kan forskningsresultaterne ikke offentliggøres.

Konklusion

Vi antager, at kravet om adskillelse af personoplysninger fra andre data kun gælder, såfremt det er muligt uden at forskertse forskningsformålet. I modsat fald vil Statsbiblioteket ikke kunne leve op til forordningens krav, da det for en række af bibliotekets samlinger gælder, ikke er muligt at anonymisere data eller opbevare dem adskilt fra de øvrige oplysninger.

Det er uklart, hvordan enkeltpersoner er stillet mht. at kunne gennemføre historisk, statistisk eller videnskabelig forskning, der inddrager

personoplysninger. Det bør tydeliggøres, at også enkeltpersoner kan gennemføre forskning, der berører personoplysninger.

Vi har stor forståelse for, at man ikke unødigt udstiller personer ved at offentliggøre følsomme eller andre private oplysninger om dem, men en bestemmelse, der kategorisk fastslår, at hensynet til den registrerede person går forud for muligheden for at fremlægge forskningsresultater, dvs. forud for hensynet til ytringsfriheden, er så vidtgående, at der må advares mod at indføre en sådan bestemmelse.

Med venlig hilsen

Svend Larsen
Direktør

DIF-sekretariat
15-06-2012

Kulturministeriet

DANMARKS IDRÆTS-FORBUND
Olympisk komite

Forlag til forordning om persondatabeskyttelse.

Justitsministeriet har i brev af 11. maj 2012 iværksat en høring over Europa-Kommissionens forslag til forordning om databeskyttelse. Kulturministeriet har videresendt høringsmaterialet og har forespurgt Danmarks Idræts-Forbund (DIF) om forbundets bemærkninger til forordningsforslaget.

Danmarks Idræts-Forbund har for nuværende en række bemærkninger, dels bemærkninger af mere almen karakter, dels bemærkninger som vedrører specifikke forhold af væsentlig betydning for DIF.

DIF finder konkluderende, at tre forhold i forordningsforslaget må ændres, hvis ikke DIF's bekæmpelsesprogrammer mod seksuelt misbrug af børn og unge mod doping skal lide skade. De tre forhold er følgende:

1. Artikel 6 bør for organisationer baseret på frivilligt medlemskab tilføres et særskilt adgang til behandling af persondata, også data af personfølsom karakter, for vedtægtsbestemte forhold i disse organisationer.
2. Samtidig bør der opstilles begrænsninger for anvendelsen af artikel 7, stk. 3 og stk. 4, så adangen til at tilbagekalde henholdsvis anfægte et givent samtykke begrænses.
3. Endelig må artikel 40-45 modificeres, så betingelserne for videregivelse af oplysninger til internationale organisationer lempes, i hvert hvad angår det internationale antidoping-arbejde.

Baggrunden for forordningsforslaget
Det anføres af Kommissionen, at der blandt interessenterne har været et udtalt ønske om, at der fastsættes et centralt regelsæt på forordningsniveau, og det anføres, at man med det foreliggende forordningsforslag søger at finde en balance mellem fornøden beskyttelse og praktisk anvendelighed.

DIF efterspørger for så vidt ikke en central EU-forordning dette retsområde. Gældende dansk lovgivning regulerer allerede området ganske detaljeret og yder en tilstrækkelig beskyttelse for den registrerede, og modsvarende opstiller lovgivningen allerede en række betingelser, som på uheldig vis begrænser eller bureaukratiserer DIF's aktiviteter på anerkendte områder med stor samfundsmæssig betydning som antidoping og pædofilibekæmpelse.

Idrættens Hus
Brøndby Stadion 20 · DK 2605 Brøndby
Tlf. +45 4326 2626 · Fax +45 4326 2628
www.dif.dk

Forordningsforslaget er vidtgående
Forordningsforslaget er ret omfattende og har en ganske kompleks karakter, og forslaget vil givetvis få omfattende konsekvenser for både offentlige myndigheder og private aktører, hvis det vedtages, som det aktuelt foreligger.

Hvor omfattende konsekvenserne bliver for DIF, er det ikke muligt at vurdere endeligt for nuværende, ikke mindst fordi rækkevidden af de foreslåede bestemmelser i høj grad vil afhænge af, hvordan en række forskellige elastiske betingelser vil blive anvendt i praksis.

Det er DIF's overordnede opfattelse, at en EU-forordning ikke må blive mere restriktiv end gældende dansk lovgivning: Som forslaget foreligger, bliver det imidlertid på en række punkter mere restriktivt end gældende lov, herunder i en grad så det kompromitterer DIF's antidopingarbejde og DIF's program for bekæmpelse af seksuelt misbrug.

DIF kan derfor ikke støtte forslaget i den foreliggende udgave.

DIF kan i øvrigt kun være enig med Justitsministeriet i, som det anføres på side 25 i ministeriets grundnotat, at der må foretages en nærmere vurdering af forslaget, før den danske regering tager endelig stilling til det. Vi vil opfordre til, at private aktører fortsat inddrages, og fra DIF's side tager vi således også forbehold for at kunne kommentere yderligere på forordningsforslaget under dets videre behandling.

Persondata i medlemsbasereder organisationer
DIF og de under DIF hørende specialforbund og foreninger håndterer persondata om sine medlemmer, også persondata af mere følsom karakter, i mange forskellige sammenhænge.

Det er et gennemgående karakteristisk træk ved organisationer som DIF og dets specialforbund og foreninger, at håndteringen af persondata i hovedsagen sker i fællesskabets og det fælles vedtagne formåls interesse. Persondata håndteres slet og ret for at drive organisationen i overensstemmelse med medlemskredsens ønsker.

Reguleringen i forordningsforslaget er derimod, som også i gældende direktiv og dansk persondatalov, i høj grad båret af en tænkning, hvor formålet med regelsættet er at balancere modstridende hensyn til forskellige aktører med modsatrettede interesser. Forordningsforslaget synes herunder at sigte mod en interessentkreds, der primært består af borgere, virksomheder og myndigheder, mens forholdene i de medlemsbaserede organisationer i civilsamfundet ikke grad er medtænkt.

Håndteringen af persondata i DIF og tilknyttede organisationer er drevet af det fælles formål og er ikke konfliktbaseret. Forordningsforslagets systematik har derfor som konsekvens, at dele af reguleringen får eller i hvert fald kan få utilsigtede konsekvenser og medføre uforholdsmæssigt store begrænsninger for organisationernes virke i forhold til medlemskredsen.

Der er i forordningsforslaget indlagt enkelte bestemmelser, som i specifikke sammenhænge modificerer begrænsningerne for medlemsbaserede organisationers virke, men det er ikke for DIF's vedkommende gennemført i tilstrækkeligt omfang, så grundproblemet består.

For kirkesamfund m.v. er der i forslagets artikel 85 taget meget vidtgående hensyn til disses selvstyre. DIF vil opfordre til, at det generelt og overordnet overvejes, om ikke tilsvarende særstatus skulle gennemføres for andre dele af civilsamfundet, f.eks. for organisationer baseret på frivilligt medlemskab, hvor håndteringen af persondata finder sted på dette helt særegent grundlag, som medlemskabet udgør.

DIF's bemærkninger til specifikke forhold
DIF har på det det specifikke niveau bemærkninger, der knytter sig til DIF's samt specialforbunds og foreningers ordinære virke og til DIF's behandling af eksklusionssager, der involverer oplysninger af personfølsom karakter.

DIF's ordinære virke
DIF's samt specialforbunds og foreningers ordinære virke som medlemsbaserede idrætsorganisationer - afvikling af de idrætslige aktiviteter i bred forstand - indebærer håndtering af mange forskellige typer persondata af harmløs og ikke-følsom karakter. Det fungerer i praksis helt problemfrit.

Denne for organisationernes virke helt nødvendige databehandling har primært hjemmel i gældende lovs § 6, stk. 1, nr. 7. Denne bestemmelse genfindes i forordningsforslagets artikel 6, stk. 1, litra f) med en anden ordlyd.

Det er absolut nødvendigt for DIF, at forordningsforslagets bestemmelse ikke medfører en begrænsning i adgangen til at behandle persondata i forhold til gældende ret efter § 6, stk. 1, nr. 7.

Alternativt og mere præcist kunne der i artikel 6, stk. 1, indsættes en bestemmelse for medlemsbaserede organisationer, der tillader persondatabehandling, der foretages af organisationen vedrørende dens vedtægtsbestemte forhold og i det omfang der behandles oplysninger om foreningens medlemmer, jf. også bemærkningerne ovenfor. Sådan bestemmelse kendes i forvejen i gældende dansk lovs § 49, stk. 1, nr. 6, om undtagelser fra forhåndsgodkendelse.

Et sådant hjemmelsgrundlag ville netop imødekomme de særegne forhold, der gør sig gældende for den medlemsbaserede organisation, som ikke mindst i Danmark er grundlaget for det idrætslige samkvem - og for den sags skyld det frivillige fællesskab om et væld af andre interesser. Det vil i øvrigt matche den klassiske opfattelse af organisationernes adgang til selvregulering.

DIF's behandling af følsomme sager
DIF behandler sager, der indeholder følsomme oplysninger af forskellig karakter, nemlig præventive eksklusionssager ved seksuelle krænkelser og sanktionering i dopingsager.

Forordningsforslagets bestemmelser om samtykke i artikel 7 udgør et problem i denne sammenhæng. Det samme gør forordningsforslagets bestemmelser i artikel 40-45 om overdragelse af oplysninger til internationale organisationer.

Misbrugssager.
DIF har for år tilbage etableret et centralt program, der skal hindre seksuelt misbrug af børn og unge i idrætsforeningernes regi. Dette sker ved, at personer, der tidligere er dømt (eller aktuelt er sigtet) for overtrædelse af straffelovens sædelighedsforbrydelser kan udelukkes fra at bestride

tillidshverv med kontakt til børn og unge. Sager herom rejses som følge af enten en børneattest med anmærkninger eller af en verserende straffesag.

Børneattester skal som bekendt indhentes i henhold til gældende lov og bekendtgørelse, mens det ikke er en lovmæssig forpligtelse at foretage en udelukkelse af personer med positive børneattester. DIF's ordning med udelukkelse er imidlertid bredt anerkendt, også således, at Danske Gymnastik- og Idrætsforeninger og Dansk Firmaidrætsforbund i år har tilsluttet sig DIF's ordning.

Attester med anmærkninger videregives fra kriminalregistret direkte til DIF for at sikre den centrale behandling af disse sager. Videregivelsen sker på baggrund af et indhentet samtykke fra den involverede person. I de nævnte eksklusionssager foretages der høring af den klub, der har indhentet børneattesten samt af det relevante specialforbund, ligesom disse parter orienteres om den følgende afgørelse. Den involverede person er ikke nødvendigvis foreningsmedlem.

Det er absolut nødvendigt for DIF, at den beskrevne ordning kan opretholdes. Med gældende lovgivning fordres samtykke, idet DIF ikke er pålagt en eksklusionsforpligtelse ved lov. Samtykkereglerne i forordningsforslaget kan blive en hindring herfor.

Dopingsager.
DIF behandler selvstændigt dopingsager efter Nationale Antidopingregler fastsat i overensstemmelse med WADA-coden. DIF er desuden sekretariat for nævnsbehandling af dopingsager inden for bredde- og motionsidrætten. Behandlingen indebærer håndtering af personfølsomme oplysninger.

I overensstemmelse med WADA-coden inddrages atletens nationale og internationale organisationer i en dopingsag, ligesom de og andre orienteres om sagens afgørelse. Det er selvsagt nødvendigt at orientere omverdenen om en dopingsanktion, hvis sanktionen skal kunne håndhæves i praksis.

Håndteringen af personfølsomme oplysninger i denne sammenhæng er baseret på to forhold: DIF's love og tilhørende reglementer, som de idrætsaktive som medlemmer har vedtaget, og til dels et samtykke fra atleterne i forbindelse med indkaldelsen til dopingkontrol.

Det er absolut nødvendigt for DIF, at dopingbekæmpelsen fortsat kan baseres på dette grundlag. Det tillader forordningsforslaget i den foreliggende udgave ikke. Samme forhold må antages at gøre sig gældende for samtlige nationale antidoping-organisationer i Europa.

Vi henviser herunder også til bemærkninger fra WADA, afgivet over for Kommissionen i forberedelsesfasen.

Artikel 7 om tilbagekaldelse af samtykke m.v.
I det omfang DIF's behandling af de nævnte sager efter forordningsforslaget måtte forudsætte et samtykke fra de involverede personer, udgør forslagets artikel 7 et problem, jf. også præamblens bemærkninger 33 og 34.. Dette forhold rækker så vidt, at samtykket principielt skal bestå i en årrække, i første omgang mindst så længe en udelukkelse er gældende, idet denne ellers ikke kan meddeles i organisationen, men i anden omgang faktisk så længe, som en potentiel gentagelsesvirkning for den pågældende forseelse løber.

Den registrerede kan efter artikel 7, stk. 3, på ethvert tidspunkt frit tilbagekalde sit samtykke, og efter stk. 4 udgør et afgivet samtykke ikke et tilstrækkeligt grundlag, hvis der består klar skævhed mellem parterne. Gældende dansk lovgivning giver ligeledes en adgang til at tilbagekalde et samtykke.

I det omfang DIF's bekæmpelsesprogrammer efter forordningsforslaget måtte forudsætte et samtykke, vil det være højst uheldigt med en sådan fri tilbagekaldelsesadgang efter artikel 7. Lignende gør sig til dels gældende med hensyn til forslaget om retten til at blive glemt.

Principielt kan en påkendt dopingmisbruger eller en udelukket træner hermed i praksis gøre sig fri af udelukkelsen ved at trække et samtykke tilbage eller ved at anfægte dets gyldighed som retsgrundlag. Dette kan potentielt ødelægge de gældende ordninger.

Det samme gør sig gældende med hensyn til det specifikke forbud i artikel 9, stk. 1, mod behandling af bl.a. genetiske data og straffedomme. Behandling af oplysninger herom er absolut nødvendig for DIF's bekæmpelsesprogrammer og behandling af sådanne data kræver et særskilt samtykke. Artikel 9, stk. 2, litra d) og j) udgør et tilstrækkeligt grundlag til at kunne opretholde de gældende ordninger. Så specifikt for denne type oplysninger og dermed for bekæmpelsesprogrammerne udgør artikel 7 også et problem.

Artikel 40-45 om videregivelse til internationale organisationer
Som nævnt skal WADA og det relevante internationale specialforbund inddrages i forbindelse med behandlingen af hver enkelt dopingsag.

Dette er fastsat i WADA-coden. Denne inddragelse og gensidige orientering er selvsagt nødvendig, hvis dopingsanktioner skal kunne håndhæves i praksis (bortset fra de højt profilerede og alment kendte tilfælde) - hemmelig sanktioner kan ikke håndhæves så at sige.

Artikel 40-45 gør det yderst vanskeligt, i praksis formentlig umuligt, at opretholde den gensidige orientering om ikendte sanktioner, og dermed undermineres hele den internationale dopingbekæmpelse under WADA. Den meget restriktive samtykkebestemmelse i artikel 44, stk. 1, litra a), gør i denne forbindelse ikke den store forskel, dels fordi et samtykke kan tilbagekaldes, dels fordi samtykket i denne forbindelse skal være i helt særlig grad oplyst.

Forordningsforslaget må ændres
I forlængelse af ovenstående må forordningsforslaget modificeres på en række punkter, såfremt det ikke skal hindre DIF's bekæmpelsesprogrammer for seksuelt misbrug og doping.

Primært kan artikel 6, som tidligere berørt, for organisationer baseret på frivilligt medlemskab tilføres en særskilt adgang for disse til at behandle persondata, også data af personfølsom karakter, for organisationernes vedtægtsbestemte forhold. Det vil gøre det muligt i vidt omfang at opretholde gældende bekæmpelsesprogrammer, og det vil i øvrigt matche den klassiske opfattelse af organisationernes adgang til selvregulering, hvorefter reguleringen af idrættens rammer overlades til idrætten selv, så længe reguleringen ikke berører tredjemands retsstilling.

Det bemærkes, at artikel 6, stk. 1, hverken i litra c) eller i litra e) hjemler behandlingerne, idet de pågældende bekæmpelsesprogrammer efter DIF's vurdering ikke umiddelbart kan siges at bero på en retlig pligt henholdsvis en pålagt opgave.

Samtidig med eller alternativt til en tilføjelse til artikel 6 må der opstilles nogle begrænsninger for anvendelsen af artikel 7, stk. 3 og stk. 4, så adangen til at tilbagekalde henholdsvis anfægte et givent samtykke begrænses. Dette gælder både for et ordinært samtykke efter artikel 6, stk. 1, litra a) og for det særlige samtykke efter artikel 9, stk. 2, litra a). Alt i det omfang forordningsforslaget måtte kræve individuelt samtykke ved DIF's bekæmpelses-programmer.

Endelig må artikel 40-45 modificeres, så betingelserne for videregivelse af oplysninger til internationale organisationer lempes, i hvert hvad angår det internationale antidoping-arbejde.

Det er af allerstørste betydning for DIF og for den sags skyld for den organiserede idræt i Europa i det hele taget, at der bliver taget hånd om disse forhold, idet forordningsforslaget ellers, som det foreligger, vil indebære en risiko for, at de omhandlede bekæmpelsesprogrammer, som klart er i samfundets interesse, ikke kan opretholdes.

DIF's bemærkninger til almene forhold.
Forordningsforslaget indeholder en række ret vidtgående, mere almene bestemmelser, som DIF også har nogle generelle bemærkninger til.

Anvendelsen af elastiske betingelser
Forslagsteksten indeholder mange elastiske betingelser for den registeransvarliges virksomhed. F.eks. kan behandling af personoplysninger finde sted, hvis det er nødvendigt for udførelsen af en opgave "i samfundets interesse", og f.eks. er et samtykke ikke tilstrækkeligt retsgrundlag, hvis der er en "klar skævhed mellem den registrerede og den registeransvarlige."

Det er vigtigt, at rækkevidden af disse elastiske betingelser i videst muligt omfang fastlægges på forhånd, så vidt det overhovedet er muligt, og de må ikke tjene til at stramme praksis i forhold til gældende dansk lov.

Administrative bøder
Forslaget lægger op til, at der administrativt kan ikendes meget store bøder for uagtsomme overtrædelser af forskrifterne.

DIF finder det ikke hensigtsmæssigt, at Datatilsynet får adgang til at fastsætte bøder udenretligt. I hvert fald må anvendelsen af sådanne bøder være forbeholdt meget grove eller gentagne overtrædelser. Vi læser artikel 79 således, at stk. 4-6 alene vedrører erhvervsvirksomheder, så DIF og andre organisationer ikke berøres af disse, men er reguleret af stk. 1-3.

Det er som minimum afgørende, at denne ordning opretholdes, at stk. 1 i Danmark vil blive praktiseret frit og uafhængigt i forhold til virksomhedsbestemmelserne i stk. 4-6, og det er tilsvarende afgørende, at Kommissionens bemyndigelse i stk. 7 ikke udvides.

Tredjemandsklage
Artikel 73, stk. 3, giver fri adgang for tredjemand til at indbringe sager om brud på datasikkerheden.

Det er i sig selv en ordning, der kan medføre store administrative byrder for tilsynsmyndighederne og også for de fra klage til klage konkret berørte registeransvarlige. Dertil forekommer det ikke rimeligt, at den eller de registrerede personer, der måtte være uden interesse i en klage, alligevel bliver inddraget i en sådan.

DIF kan ikke støtte denne ordning.

Dokumentationskrav
I artikel 28 fastsættes ret omfattende dokumentationskrav til registeransvarlige. Der skal opbevares dokumentation for enhver behandling, der gennemføres af den registeransvarlige. Taget på ordet og læst i en dansk kontekst er dette endda uhyre omfattende.

Efter bestemmelsens stk.4 gælder dokumentationskrav dog ikke organisationer med under 250 ansatte. Det er efter DIF's opfattelse ikke helt oplagt, hvorfor undtagelsen er knyttet til organisationens størrelse. Det ville være mere nærliggende at knytte den til organisationens formål eller lignende.

DIF kan leve med den foreliggende udformning af bestemmelse. Det er imidlertid vigtigt, at undtagelsen opretholdes, og at Kommissionens beføjelse efter bestemmelsen stk. 5 ikke udvides, og at Kommissionen således ikke har bemyndigelse til at fastsætte bestemmelser, der afviger fra stk. 4.

Godkendelse af behandlingen
Artikel 34 pålægger den registeransvarlige at indhente forhåndstilladelse inden behandlingen af personoplysninger påbegyndes.

Gældende dansk lov undtager en række registre fra hovedreglen om forhåndsgodkendelse, herunder undtages i § 49, stk. 1, nr. 6, persondatabehandling, der foretages af en forening eller lignende, i det omfang der alene behandles oplysninger om foreningens medlemmer. Tilsvarende undtagelsesbestemmelser bør indføres i forordningsforslaget eller alternativt tillades gennemført nationalt.

I modsat fald vil tilsynsmyndigheden forventeligt stå med en uløselig opgave, i et land hvor antallet af alene idrætsforeninger med medlemsregistre, der principielt skal godkendes, udgør måske samlet set 15.000.

Med venlig hilsen

Karl Chr. Koch
Direktør

Morten Daniel Dahm-Hansen

Fra: Anti Doping Danmark [info@antidoping.dk]
Sendt: 15. juni 2012 10:39
Til: Helene Nordborg Kiær
Cc: Martin Holmlund Lauesen; Camilla Vange Mynster; Lone Hansen
Emne: Vedr.: Høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse
Vedhæftede filer: [Untitled].pdf

Kære Helene Nordborg Kiær

Idet vi henviser til Kulturministeriets fremsendelse af høringsmateriale vedrørende Europa-Kommissionens forslag til forordning om databeskyttelse, fremsendes herved Anti Doping Danmarks bemærkninger:

Anti Doping Danmark har en lovmæssig forpligtelse til at udføre antidopingaktiviteter i overensstemmelse med World Anti-Doping Code (WADC) i dansk idræt. Dette sker i henhold til Nationale antidopingregler for eliteidrætten og i henhold til Motionsdopingreglementet for motionsidrætten i Danmark. Herudover udføres aktiviteter i henhold til samarbejdsaftaler med relevante parter uden for den organiserede idræt i henhold til §9 i Lov om fremme af dopingfri idræt.

I denne forbindelse har ADD behov for at kunne indsamle, behandle og videreformidle (personfølsomme) data med relevante parter - både nationalt og internationalt med parter i og uden for Europa. Behandling og videreformidling af data er en forudsætning for udøvelse af vores aktiviteter. Det er absolut nødvendigt for Anti Doping Danmark, at forordningsforslagets bestemmelser ikke medfører en begrænsning i adgangen til at behandle persondata i forhold til det retsgrundlag, der gælder i dag for databehandling. (direktiv 95/46/EF og persondataloven).

Anti Doping Danmark har umiddelbart følgende konkrekte bemærkninger til forslaget:

- Eftersom samtykke ikke længere anses som lovligt retligt grundlag er det absolut afgørende for Anti Doping Danmarks virke, at databehandling kan ske med hjemmel i artikel 6, stk. 1 c) ifølge hvilken databahandling anses for lovlig, såfremt "behandlingen er nødvendig for at overholde en retlig forpligtelse, som gælder for den registeransvarlige." Det bemærkses dog, at antidopingorganisationer, der ikke har en tilsvarende lovmæssig hjemmel og for hvem samtykke i dag er det eneste retlige grundlag for databehandling, må have anden hjemmel til databehandling sådan at effektivt internationalt antidopingarbejde kan gennemføres.

- I forhold til udveksling af oplysninger med relevante internationale parter i og uden for EU, er det absolut afgørende, at der etableres hjemmel til dette, såfremt ADDs retlige forpligtelse alene ikke giver hjemmel til denne udveksling, sådan som det anses for tilfældet mht. indsamling og registrering af data, jvf ovenstående. Vi kan ikke længere basere os på udøverens samtykke idet dette samtykke ifølge forordningsforslaget ikke længere vil være tilstrækkeligt.
- Iflg. forordningsforslagets artikel 7 stk. 3 kan den registrerede på ethvert tidspunkt og uanset årsag tilbagekalde sit samtykke. (gælder også i dag) Forud for en dopingkontrol afgiver en idrætsudøver et samtykke om, at han er indforstået med at han skal testes i henhold til gældende regler og er forpligtet til at aflægge en dopingprøve. Uden at ADD har mulighed for at vurdere konsekvenserne af en sådan fri tilbagekaldelsesadgang bemærkes det, at procedurer for dopingkontrol og sanktionering skal kunne ske i henhold til gældende regler uden begrænsning af en eventuel tilbagekaldelse af samtykke.

Der henvises i øvrigt til de bemærkninger WADA har indsendt til Kommissionen i forbindelse med udarbejdelsen af forslaget. (se vedhæftede)

Med venlig hilsen

Christina Friis Johansen

Anti Doping Danmark
Idrættens Hus
Brøndby Stadion 20
2605 Brøndby

Tel. Dir. +45 4326 2522
Mob.tel +45 4031 3106

WORLD
ANTI-DOPING
AGENCY
play true

WORLD ANTI-DOPING AGENCY

EUROPEAN COMMISSION CONSULTATION: THE LEGAL FRAMEWORK FOR THE FUNDAMENTAL RIGHT OF PERSONAL DATA

I. INTRODUCTION

The World Anti-Doping Agency ("WADA") appreciates the opportunity to respond to the European Commission's consultation focusing on the effectiveness of EC Directive 95/46/EC (the "Directive"). WADA is an independent international agency established in 1999, and is composed and funded by the sports movement and governments around the world. WADA's mission is to foster and promote a doping-free culture in sport. To that end, WADA conducts scientific research, offers education and awareness programs, contributes to the development of anti-doping practices and monitors implementation of the World Anti-Doping Code (the "Code") – the document harmonizing anti-doping practices worldwide for sport. WADA also produced in 2009 the first global data protection standard, the International Standard for the Protection of Privacy and Personal Information (the "Standard").

WADA's mission of implementing anti-doping controls in organized sport, and its creation of the Standard, has brought it into regular discussions with the various bodies overseeing Europe's data protection regime, including the Council of Europe, the Article 29 Working Party and national data protection regulators. More recently, the Standard and anti-doping practices more generally were the subject of two opinion papers published by the Article 29 Working Party.[1] This experience has given WADA a unique insight into how European data protection regulators interpret certain provisions of the Directive, as well as convinced it of the need to submit this response. Indeed, WADA fears that some regulators are engaging in an overly restrictive interpretation and application of EU data protection rules and thereby threatening to undermine the very anti-doping programs that Europe, both at the Community and local level, has been promoting and supporting around the world for many years.

[1] *See* WP 162 (adopted 6 April 2009); WP 156 (adopted 1 August 2008). WADA's formal response to the Article 29 Working Party papers, and other relevant materials, can be found on WADA's website at: www.wada-ama.org.

Stock Exchange Tower, 800 Place Victoria (Suite 1700), PO Box 120 – Montreal (Quebec) H4Z 1B7 Canada
Tel: + 1 514 904 9232 ◊ Fax: + 1 514 904 8650
www.wada-ama.org

Community instruments, as well as numerous Commission policies and public statements, repeatedly recognize the importance of the fight against doping in sport and the substantial public interest that anti-doping efforts serve. The Commission's recent *White Paper on Sport* (COM (2007) 391) refers to the serious threat doping in sport poses to individual and public health, as well as the image of sport.[2] Meanwhile, the Treaty of Lisbon has enshrined into European law the aim of "protecting the physical and moral integrity of sportsmen and women," an aim directly advanced by European anti-doping regimes, and nearly all Member States have ratified both the Council of Europe's *Anti-Doping Convention* (ETS No. 135) and the United Nations' *International Convention Against Anti-Doping in Sport*.

Given the above, the Commission's consultation represents a critical opportunity for Europe to ensure that its data protection framework, and Directive 95/46/EC in particular, is not brought into needless conflict with European anti-doping efforts. WADA continues to believe that this framework can accommodate modern anti-doping practices when sensibly applied by national regulators. It has even prepared and published a number of detailed submissions on this point. For purposes of this response, WADA simply will concern itself with features of Directive 95/46/EC that could be updated to take account of modern anti-doping programs and reduce the possibility of conflicts between anti-doping practices and data protection rules arising in future.

II. PROPOSED AMENDMENTS TO DIRECTIVE 95/46/EC

1. Amend Article 8 to provide an explicit legal basis for the processing of sensitive data by anti-doping organizations.

WADA would urge the Commission to propose amending Article 8, governing the processing of sensitive personal data, to provide a much clearer legal basis for the processing of such data by European anti-doping organizations. By way of background, anti-doping organizations routinely collect and process health information relating to athletes in the normal course of administering their anti-doping programs. For instance, athletes may submit requests to use banned substances for a documented therapeutic use or have their biological samples analyzed in connection with in and out-of-competing testing. Anti-doping organizations thereby acquire a significant amount of information relating to the health of athletes.

---

[2] See, in particular, the Commission's "Staff Working Document" accompanying the *White Paper*, which refers to the fact that doping represents a threat to, among other things, individual and public health (especially for children and young people), the principle of open and equal competition, and the image of sport.

To be clear, WADA believes that European anti-doping organizations should be able to rely on existing Article 8 provisions, such as Article 8(2)(a) (consent), when processing such data. But, WADA's experience is that certain European data protection regulators challenge this view. Consequently, except in those Member States that have enacted legislation expressly addressing the processing of sensitive athlete data by anti-doping organizations, a clear legal basis for such processing often appears to be lacking. This "legislative solution," moreover, cannot be the preferred solution. Expecting Member States to enact local laws would be inconsistent with the aim of the Commission's own *White Paper on Sport* and the terms of the Treaty of Lisbon, both of which call for a more coordinated "European" approach to doping and action at the EU - not Member State - level.[3]

We therefore think the Commission should consider creating alternative legitimate grounds for the processing of sensitive data by anti-doping bodies, both public and private. On the one hand, this could be achieved by expanding existing Article 8(3) of the Directive to explicitly permit the processing of sensitive athlete data by anti-doping organizations. Article 8(3) excludes the application of Article 8(1) in cases where health information is processed by medical professionals subject to a professional duty of confidentiality or by others subject to a comparable duty. We suggest extending Article 8(3) to allow "processing of sensitive data performed by competent national or international anti-doping authorities required for the purposes of conducting anti-doping procedures on athletes participating in organized sport," provided such processing is performed by persons subject to a professional duty of confidentiality (e.g., medical professionals) or its equivalent.[4]

Alternatively, the same result might be achieved by amending Article 8(2)(d), which permits foundations, associations and non-profit bodies to process sensitive data relating to their own members or other persons with a close connection with those entities. Amending Article 8(2)(d) to expressly include the processing of sensitive data by anti-doping organizations represents a logical extension of the provision to a closely analogous context, one that the original drafters of Directive 95/46/EC may not have considered. Anti-doping organizations similarly gather information from and about their "members" (i.e., the athletes who have registered with the organization) and ensure that they

---

[3] The Treaty of Lisbon, for instance, calls for Union action aimed at "developing a European dimension in sport, by promoting fairness and openness in sporting competitions and cooperation between bodies responsible for sports, and by protecting the physical and moral integrity of sportsmen and sportswomen, especially the youngest sportsmen and sportswomen." *See* Article 165(2).

[4] Alternatively, language similar to that found in Article 13(1)(d) and (f) of the Directive could be used. This might help solve a potential second problem that might arise where certain data protection authorities engage in an expansive interpretation of Article 8(5) to treat certain anti-doping data – namely, that data indicative of a doping violation – as "judicial data."

adhere to rules of appropriate conduct when training for or competing in events and competitions, including compliance with a strict anti-doping code that guarantees a level playing field for all.

That said, Article 8(2)(d), as now drafted, provides that the covered entities also must refrain from disclosing the relevant "membership" data to third parties without the consent of the data subject. This particular condition will prove problematic in the anti-doping context given the open hostility shown by European data protection regulators to reliance on consent to justify the processing of sensitive data, both generally and specifically in the anti-doping context, and the fact that European anti-doping organizations routinely need to disclose data to other anti-doping organizations (in Europe and elsewhere). For this reason, any proposal tabled by the Commission would need to eliminate the need to secure data subject consent to third party disclosures (or provide for other options) or else the proposed amendment would be of little practical benefit.

Third, and last, the Commission could investigate whether some of the legal bases that now appear under Article 7, perhaps combined with proposals for heightened security, new audit and transparency requirements, greater oversight by data protection authorities or expanded user control, could be sensibly incorporated into Article 8.[5] For instance, one possibility would be to permit processing carried out in the public interest, as now appears at Article 7(e). That anti-doping serves such interests is clear, as we note above. This has even been affirmed by the European Court of Justice, which observed in *Meca-Medina* (Case C-519/04 P) that combating doping is necessary to safeguard both the health of athletes, the integrity and objectivity of competitive sport and the ethical values in sport.

2. Revise Article 26 to enable anti-doping organizations to transfer personal data where necessary in connection with their legitimate anti-doping activities.

WADA would urge the Commission to propose amending Article 26, establishing derogations to the general transfer restrictions contained at Article 25, to facilitate the transfer of personal data by anti-doping organizations in connection with their anti-doping programs. This is necessary because, at present, some European data protection regulators appear to question the basis upon which such data may be legitimately transferred by European anti-doping organizations to other anti-doping bodies outside the European Union. In the

[5] Article 8(4) even permits Member States and data protection regulators to create exemptions to permit the processing of sensitive data - something they cannot do for ordinary personal data under Article 7. The result is that European data controllers are subject to divergent Member State approaches to the regulation of sensitive personal data.

absence of a clear legal basis, some European anti-doping organizations are uncertain as to whether they may lawfully transfer such data.

That European anti-doping organizations need to transfer such data is clear. For example, when athletes in the registered testing pools of these organizations train or compete in a foreign country, their whereabouts data often needs to be shared with local anti-doping authorities in order to allow them to perform in- or out-of-competition testing. If relevant data cannot be shared with competent anti-doping authorities in these circumstances, it is easy for an athlete to simply circumvent the rules and evade doping tests. Further, European anti-doping organizations may collect data on foreign (i.e., non-EU) athletes competing or training in Europe, and will need to disclose the results of any anti-doping tests they conduct with the foreign anti-doping organizations with whom the athletes are registered.

Again, WADA's position is that Member States and their national data protection regulators could allow such transfers using one of the existing derogations at Article 26. Further, representations made by the Canadian data protection authorities reveal that anti-doping data, including personal data, uploaded onto WADA's anti-doping database located in Canada, known as ADAMS, are subject to adequate protection (in the Article 25 sense) by virtue of applicable Canadian federal and provincial privacy laws. For other international transfers, WADA believes that the sensible application of Article 26(1)(a) (consent), 26(1)(c) (fulfillment of contracts) or Article 26(1)(d) (public interest) could apply in the anti-doping context, although some regulators are sceptical.[6] This is unfortunate, as most athletes themselves often wish to participate in such controls to demonstrate their adherence to the World Anti-Doping Code and commitment to doping-free sport.

Ultimately, European anti-doping organizations and athletes should be afforded a clearer legal basis legitimizing the international transfer of such data. WADA can envision at least two possible solutions to this problem arising from the current restrictive interpretation and application of Article 26. First, Article 26(1) could be amended to specifically permit transfers of personal data by European anti-doping organizations "where necessary to perform anti-doping controls" (or language having an equivalent effect). Second, and alternatively, the Commission could propose amending Article 26(4) to allow transfers not only where the Article 31 Committee concludes that particular contractual clauses provide adequate safeguards, but also where industry codes or standards do so

[6] Some have suggested reliance on other measures, such as contracts, to transfer athlete personal data. Such a suggestion is unsuited to the anti-doping context given that athletes can compete and train in a multitude of countries, often at short notice, and anti-doping organizations processing the data can be public bodies unwilling or unable to execute data transfers agreements. This was even acknowledged by the Swiss Federal Data Protection Authority in its 15th Annual Report (2007/2008).

as well. It is unclear why Article 26(4) only permits the Article 31 Committee to consider contractual controls, when it is clear that adequate protections can also be adduced through other mechanisms, such as codes, standards or even "binding corporate rules."

WADA considers the above suggestion concerning Article 26(4) relevant to anti-doping, insofar as there currently exists – in the form of the WADA International Standard for the Protection of Privacy and Personal Information – an effective and robust data protection standard that governs the activities of anti-doping bodies worldwide and creates a high level of protection for personal data processed by such bodies. WADA's Standard meets, and very often exceeds, the level of protections provided for by the International Privacy Standard endorsed by the global privacy community, including European authorities, at the recent Privacy Commissioners' Conference in Madrid, Spain. In WADA's opinion, it would be an easy step for the Article 31 Committee to conclude that the Standard, either as it exists now or with certain provisions amplified, provides a sufficiently high level of protection to warrant its own adequacy determination.

* * *

WADA once again would like to thank the European Commission for this opportunity to make its views on EC Directive 95/46/EC known. WADA would be pleased to discuss its suggestions with the Commission in more detail, should that be helpful.

Kulturministeriet
Kulturbevaring
Nybrogade 2
1203 København K
Att.: Helene Nordborg Kiær
Maj Vestergaard K-Hafstrøm

København, den 15. juni 2012

Vedr. høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse

Ved e-mail af 8. juni 2012 har Kulturministeriet anmodet om eventuelle bemærkninger til det fremsendte høringsmateriale.

Gramex har med stor interesse gennemgået høringsmaterialet, men har ikke fundet anledning til at komme med kommentarer hertil.

Med venlig hilsen

Grace Nguyen Suhadi
Juridisk konsulent
Forretningsudvikling

STATENS ARKIVER

RIGSARKIVET

Kulturministeriet
kum@kum.dk

Dato:	*Journalnummer:*	*Lokaltelefon:*	*Vores reference:*	*Deres reference:*
15. juni 2012	*2012-012554*	*41717246*	*JDS/PO-AHE*	

Vedr. forslag til ny forordning om personoplysninger

Kulturministeriet har anmodet Statens Arkiver om bemærkninger til "Forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)" .

Statens Arkiver finder, at forslaget i sin nuværende udformning indebærer en række alvorlige problemer i forhold til Statens Arkivers virke.

Statens Arkivers formål er at sikre bevaringen af arkivalier, der har historisk værdi og at stille sådanne arkivalier til rådighed for myndigheder, offentlighed og forskning. Disse formål opfyldes i dag gennem modtagelsen af de arkivalier, der skabes af den offentlige forvaltning. I dag består hovedparten af de modtagne arkivalier af dataudtræk fra forvaltningens it-systemer, som i sagens natur indeholder personoplysninger i struktureret form. Digitale arkivalier uden oplysninger, der kan henføres til fysiske personer, hører til undtagelserne.

Statens Arkivers virksomhed, for så vidt angår digitale arkivalier med personoplysninger, har hidtil været reguleret af persondataloven og arkivlovgivningen. Vigtigst i denne forbindelse er persondatalovens § 14, der fastsætter, at oplysninger, der er omfattet af persondataloven, kan overføres til opbevaring i offentlige arkiver efter reglerne i arkivlovgivningen.

Persondataloven implementerer Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. I dette direktiv findes en række henvisninger til den behandling af personoplysninger, der finder sted i forbindelse med historiske, statistiske eller videnskabelige undersøgelser. Behandling af personoplysninger med historisk, statistisk eller videnskabeligt kan således lovligt finde sted, for så vidt den nationale lovgivning fastsætter de fornødne sikkerhedsgarantier.

Rigsdagsgården 9 · dk-1218 København K
Telefon: (+45) 33 92 33 10 · Telefax: (+45) 33 15 32 39
E-mail: mailbox@ra.sa.dk · Hjemmeside: www.sa.dk

I det foreliggende forordningsforslag er henvisninger af denne karakter ikke videreført. Dette indebærer en risiko for, at den praksis, der har fundet sted efter arkivlovens og persondatalovens bestemmelser, ikke vil være lovlig, om forordningsforslaget gennemføres.

I udarbejdelsen af forordningsforslaget synes i det hele ikke den sekundære udnyttelse af administrativt indsamlede data til forskningsformål at være overvejet fra et forskningsmæssigt synspunkt.

Artikel 83 omhandler behandling af personoplysninger til historiske, statistiske eller videnskabelige forskningsformål. Artiklen indebærer en meget vidtgående overdragelse til Kommissionen af beslutningskompetence på områder, som hidtil har været reguleret af medlemsstaternes egen lovgivning, her i landet persondataloven og arkivloven.

Artiklens stykke 1 synes at betyde, at data *enten* skal anonymiseres *eller* opbevares i en form, således at identifikationsoplysningerne opbevares adskilt fra øvrige oplysninger. En væsentlig del af den historiske og forskningsmæssige værdi i de arkiverede data i Statens Arkivers samlinger er netop, at de i høj grad indeholder eksempelvis CPR-numre, som muliggør forskning på tværs af datasæt og arkivalietyper.

Ved en anonymisering ville man således miste en overordentlig stor del af de forskningsmæssige genanvendelsesmuligheder. Alternativet at adskille de oplysninger, som identificerer personer, fra de øvrige oplysninger ville betyde opbygningen af et meget kompliceret system, hvor oplysninger skulle adskilles ved modtagelse i Statens Arkiver, opbevares separat og derefter på en sikker og troværdig måde kunne sammenstilles igen ved forskningsmæssig brug. En sådan løsning ville være prohibitivt dyr at udvikle og administrere, hvis det overhovedet var muligt at gennemføre sådant indgreb i data uden meget alvorlige konsekvenser for datas autenticitet, integritet og muligheden for samkøring ved tilgængeliggørelse. Den forskningsmæssige værdi af data kan reduceres i en grad, der gør bevaringen ligegyldig.

Artiklens stykke 2 betyder, at arkivalier med personoplysninger kun må tilgængeliggøres, hvis en af tre følgende betingelser er opfyldt:

- den registrerede har givet sit samtykke
- offentliggørelsen er nødvendig for at fremlægge forskningsresultater eller fremme forskningen
- den registrerede har selv offentliggjort oplysningerne.

Samtykke fra den registrerede er ikke mulig, idet de registrerede personer på det tidspunkt, hvor oplysningerne bliver alment tilgængelige iht. arkivloven, i langt de fleste tilfælde vil være afgået ved døden. Lige så absurd er det at forestille sig, at borgerne ved afgivelse af selvangivelse, indlæggelse på sygehus, modtagelse af en dom eller en af de talrige andre situationer, der afspejler sig i den offentlige forvaltnings registre skal give tilsagn om, at disse oplysninger i en fjern fremtid må offentliggøres. En "tilsagns"-løsning ift. offentliggørelse af data fra offentlige registre er i praksis umulig.

En offentliggørelse af data, der baserer sig på en kontrol af, om den registrerede selv har offentliggjort oplysningerne, er i sagens natur ligeledes umulig.

Statens Arkiver kan derfor kun, iht. forslaget, offentliggøre personoplysninger, såfremt det er nødvendigt for fremlæggelse af forskningsresultater eller fremme forskningen. Af forslaget fremgår det ikke, hvilke kriterier, der skal være opfyldt, og der foreligger ingen tidsgrænse for, hvornår data evt. kan stilles generelt til rådighed for forskning. Det skal i den forbindelse bemærkes, at arkivalier med personoplysninger i dag først bliver umiddelbart tilgængelige efter 75 år iht. arkivlovens § 23, stk. 1.

Artiklens stykke 3 indebærer, at kompetencen til at fastlægge nærmere kriterier for opfyldelse af bestemmelserne i stk. 1 og 2 flyttes til EU-kommissionen. Kommissionens delegerede retsakter vil have umiddelbar retsvirkning i medlemslandene.

Forslaget vil således medføre en situation, hvor de data som opbevares i Statens Arkiver og andre offentlige arkiver er underlagt EU's databeskyttelsesregler. Det vil være Kommissionen, der træffer afgørelse om, hvilke kriterier der skal være opfyldt for, at offentliggørelse af personoplysninger er "nødvendig". Det er en meget vidtgående ændring af gældende retstilstand.

Det skal i den forbindelse bemærkes, at forslaget blev drøftet indgående af de europæiske rigsarkivarer på mødet i EBNA (European Board of National Archivists) i København i maj måned. Der er blandt de europæiske arkiver er en klar og fælles bekymring for forslagets betydning for arkivernes mulighed for også fremadrettet at bevare og tilgængeliggøre historisk dokumentation.

Udover de nævnte problemer med artikel 83, indebærer forslaget yderligere en række uhensigtsmæssigheder, som følger af, at der ikke i fornøden grad er taget højde for den særstilling, som må gælde for opbevaring af data til historiske m.v. formål:

Eksempelvis artikel 15 om den registreredes ret til indsigt. I den danske arkivlov er data, som opbevares i offentlige arkiver ikke undtaget fra regler om egenindsigt, men egenindsigten gennemføres efter en særlig procedure, jf. arkivlovens § 42. Skulle Statens Arkiver som dataansvarlig gennemføre egenindsigt efter samme regler som de myndigheder, der oprindeligt har registreret oplysningerne, ville det indebære meget betydelige omkostninger.

Artikel 17 om "Ret til at blive glemt og ret til sletning" gælder ikke for data, der opbevares til historiske, statistiske eller videnskabelige forskningsformål, men formuleringen af artiklens stykke 4 tyder på, at bevaringsinstitutioner kan blive tvunget til at foretage ændringer i arkiverede data, med mindre man kan dokumentere, at data er korrekte. For data, der er indsamlet fra hele den offentlige forvaltning siden 1970'erne vil dette selvsagt være et krav, som ikke kan opfyldes.

Konklusion
Forslaget stiller krav til opbevaring af personoplysninger, som vil pålægge de offentlige arkiver meget store ekstraomkostninger og medføre alvorlige risici for arkivaliernes integritet og autenticitet. Det

pålægger endvidere arkiverne krav om indsigtsret m.v., som kun med meget store økonomiske ressourcer, om overhovedet, ville kunne gennemføres i praksis.

Endelig overdrager forslaget al kompetence til at fastsætte regler med stor rækkevidde for de offentlige arkivers virksomhed til EU-kommissionen. Statens Arkiver finder, at spørgsmålet om aflevering, bevaring og tilgængelighed til data, der opbevares af historiske, statistiske eller videnskabelige forskningsformål, mest hensigtsmæssigt fastlægges i den nationale lovgivning, hvor de nødvendige garantier til sikring af borgernes rettigheder, beskyttelsen af privatlivets fred mv. kan fastsættes, som det hidtil uden ulemper har fundet sted.

Med venlig hilsen

Asbjørn Hellum
Rigsarkivar

Morten Daniel Dahm-Hansen

Fra: Morten Brustad [MOB@danskerhverv.dk]
Sendt: 18. juni 2012 10:07
Til: Helene Nordborg Kiær
Cc: Pernille Lethare Madsen
Emne: SV: Høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse

Kære Helene Nordborg Kiær.

Hermed fremsendes DFHOs bemærkninger til nævnte høring.

DFHO har i henhold til gældende lovgivning i 2008 indgået en aftale med Anti Doping Danmark vedrørende kontrol og oplysning gældende for samtlige medlemmer af DFHO og omfatter samtlige kunder i et DFHO medlemscenter

For så vidt angår kontrol foretager Anti Doping Danmark vilkårlige test af personer, der træner i et DFHO medlemscenter. Såfremt disse testes positive eller nægter at få udført en test, skal der i henhold til aftalen gives den pågældende en sanktion i form af udelukkelse fra træning i samtlige DFHO centre.

For at kunne iværksætte en effektiv sanktion over for den pågældende registreres den pågældende på en liste. Denne liste videregives til samtlige medlemscentre af DFHO, som herefter kontrollerer alle nye kunder i forhold til eventuel sanktion i form af udelukkelse.

I det omfang forordningen om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger indeholder ændringer og nyskabelser, der påvirker DFHOs adgang til at videregive oplysninger fra Anti Doping Danmark om positive test eller nægtelser af test til samtlige medlemmer af DFHO, skal DFHO bemærke, at man har en væsentlig interesse i at kunne fastholde adgangen til denne videregivelse.

Denne interesse udgør hele fundamentet for Anti Doping Danmarks kontrol program og er derfor en afgørende forudsætning for den nuværende frivillige model for bekæmpelse af dopingmisbrug i motionsidrætten.

I forlængelse af Kulturministeriets rapport om kontrol af dopingmisbrug af motions- og fitnesscentre skal det tilføjes at samme interesse på tilsvarende måde efter DFHOs opfattelse udgør hele fundamentet for en kommende og endnu mere effektiv indsats mod misbrug af doping i motionsidrætten i forhold til videregivelse af oplysninger på tværs af idrættens aktører og i forhold til etablering af en centralt register i Anti Doping Danmark, som alle kan benytte sig af.

Med venlig hilsen

Morten Brustad
Sekretariatschef advokat

MOBIL: +45 2088 3247
DIREKTE: +45 3374 6407
MOB@DANSKERHVERV.DK

DANSK ERHVERV

Dansk Erhverv er erhvervsorganisation og arbejdsgiverforening for fremtidens erhverv. Vi repræsenterer 17.000 virksomheder og 100 brancheorganisationer inden for handel, rådgivning, oplevelse, transport og service.

DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
F. +45 3374 6080
CVR NR. 43232010
INFO@DANSKERHVERV.DK

Morten Daniel Dahm-Hansen

Fra: Maria Fredenslund [maria@rettighedsalliancen.dk]
Sendt: 18. juni 2012 15:45
Til: Helene Nordborg Kiær
Cc: Maj Vestergaard K-Hafstrøm
Emne: SV: Høring over Europa-Kommissionens forslag til generel forordning om databeskyttelse

Kære Helene

Tak for muligheden for at bidrage med input til Kulturministeriets høringssvar vedrørende Kommissionens forslag til generel forordning om databeskyttelse. I lyset af den korte tidsfrist er vores input fokuseret på enkelte områder og enkelte generelle kommentarer. I er selvfølgelig meget velkomne til at vende tilbage, hvis der er yderligere områder, som I umiddelbart ønsker vores bemærkninger til.

RettighedsAlliancen behandler data om personer, der mistænkes for at have overtrådt ophavsretsloven. Behandlingen sker dels med henblik på at fastlægge et retskrav herunder vurdere, om der er grundlag for retsforfølgelse, og dels med henblik på at indgive politianmeldelse eller forfølge sagen civilretligt. De data, der behandles, er som udgangspunkt ikke-følsomme data, men når de (via domstolene) kædes sammen med oplysninger, der danner grundlag for en mistanke om overtrædelse af ophavsretsloven, da fører dette til, at oplysningerne overgår til at være følsomme data, jf. persondatalovens § 8, stk. 4. Datatilsynet har givet tilladelse til den omtalte behandling.

Følgende temaer i Kommissionens forslag giver umiddelbart anledning til bemærkninger:

- Betingelserne for et gyldigt samtykke til behandling af persondata
- Betingelserne for behandling af persondata
- Databehandlerens ansvar

Om betingelserne for et gyldigt samtykke til behandling af persondata
Artikel 7 (og artikel 4(8) og betragtningerne 25,33 og 34) definerer betingelserne for et gyldigt samtykke og betingelserne er strammet væsentligt i forhold til det gældende direktiv. Samtykket skal være givet udtrykkeligt fra den fysiske person, der er subjekt for behandling af persondata. Der skal være tale om en erklæring eller en positiv handling - stiltiende samtykke eller undladelseshandlinger kan derfor ikke udgøre samtykke.

Sådanne øgede krav indebærer nødvendigvis mere bureaukrati for dataansvarlige og databehandlere.

Om betingelserne for behandling af persondata
Betingelserne for behandling af persondata foreslås indskrænket. Forslagets artikel 6(1)(f) (om lovlig behandling) er genstand for flere restriktioner end det nugældende direktivs artikel 7(f) (Direktiv 95/45EF). Listen over følsomme data foreslås udvidet, jf. forslagets artikel 21, som modsvarer det nugældende direktivs artikel 13. Det foreslås derudover, at Kommissionen bemyndiges til at vedtage "delegerede retsakter" (forslagets artikel 6, stk. 5), som specificerer flere betingelser eller elementer, der kan indgå i afvejningen af, om hensynet til den dataansvarliges interesser i at behandle personoplysninger, overstiger den registreredes interesser. Samme bemyndigelse foreslås indført i forhold til behandling af personfølsomme data (forslagets artikel 9, stk. 3).

Det konkrete indhold og rækkevidden af Kommissionens bemyndigelse, jf. forslaget artikel 6, stk. 5 og artikel 9, stk. 3, er ikke fastlagt. En sådan vedvarende mulighed for Kommissionen til at vedtage nye og ændre eksisterende retsakter medfører, at direktivets indhold og rammer vil indebære en væsentlig grad af retlig uforudsigelighed og usikkerhed for dataansvarlige og databehandlere. Det synes også at være i modstrid med direktivets formål om at "fremme(r) retssikkerheden og den retlige klarhed", "klare regler" og "en stærk og konsekvent retlig ramme" (Kommissionens meddelelse af 25. januar 2012, hhv. side 2, 12 og 4).

Indskrænkningerne i betingelserne for behandling af persondata vil i det hele taget gøre det vanskeligere at behandle persondata med henblik på efterforskning og retsforfølgelse. Også af denne grund er det væsentligt, at der

i artikel 21 opretholdes den specifikke henvisning til "*beskyttelse af* den registreredes interesser eller *andres rettigheder* og frihedsrettigheder.", jf. artikel 21 (1)(f) (min fremhævning). Denne bestemmelse vil formentlig fortsat være et væsentligt bidrag til at fastsætte berøringsfladerne mellem beskyttelse af privatlivets fred og beskyttelsen af ophavsrettigheder. Dog virker det ikke umiddelbart hensigtsmæssigt, at bestemmelsen alene er en undtagelse til artikel 5 men ikke til artikel 6 (om lovlig behandling).

Om databehandleres ansvar
Ansvar og pligter for databehandlere og dataansvarlige er blevet meget mere omfattende med forslaget end i det nugældende direktiv. Databehandlingen skal være omfattet af en kontrakt som indeholder en række elementer, der er oplistet i forslagets artikel 26(2). Dataansvarlige og databehandlere skal opbevare dokumentation for alle behandlinger af data under den pågældendes ansvar. Dokumentationen skal indeholde en række information, der er oplistet i forslagets artikel 28(2). Kommissionen vil også her være bemyndiget til at vedtage yderligere delegerede retsakter samt retsakter i forbindelse med implementering.

En sådan udvidelse af ansvar og pligter vil selvsagt påføre yderligere administration mm. på dataansvarlige og databehandlere. Kommissionens bemyndigelse til at vedtage yderligere regler medfører som i de øvrige tilfælde, hvor Kommissionen er tillagt denne beføjelse, retlig uforudsigelighed og usikkerhed for de, der behandler persondata.

Generelle bemærkninger
Det er bekymrende, at forordningsforslaget ikke indeholder en specifik henvisning til ejendomsret herunder intellektuel ejendomsret (enten i en artikel eller i en betragtning). En sådan henvisning bør tilføjes. Den omtalte meddelelse fra Kommissionen henviser til "retten til at drive virksomhed" (fx side 23), men der findes ingen tilsvarende reference i forslaget. Også i lyset af retspraksis fra EF Domstolen herunder den nyere dom om Scarlet vs. Sabam, vil det være hensigtsmæssigt at indføre en sådan tilføjelse.

Idet initiativet formentlig efter hensigten vil medføre en øget harmonisering af reglerne i de enkelte medlemsstater, er det tvivlsomt, om det vil forbedre retssikkerheden. Mange regler og rammer er genstand for yderligere delegerede retsakter, hvilket vil være forbundet med retlig usikkerhed for de involverede dataansvarlige og databehandlere.

Endelig er det bekymrende, at grænsefladerne mellem retten til privatlivets fred og beskyttelsen af intellektuelle ejendomsrettigheder ikke er blevet tydeliggjort med dette forordningsforslag. Det havde været nærliggende at tydeliggøre - særligt i lyset af seneste retspraksis fra Domstolen.

I er meget velkomne til at vende tilbage med evt. spørgsmål, bemærkninger eller andet.

Venlig hilsen
Maria

Maria Fredenslund
Leder og talsmand for RettighedsAlliancen

Direkte: +45 - 32 71 20 62
Mobil: +45 – 21 64 74 48
E-mail: maria@rettighedsalliancen.dk
Tel: +45 - 32 71 21 21
Fax: +45 - 32 71 21 00
Web: www.rettighedsalliancen.dk
RettighedsAlliancen
Højbro Plads 10
DK-1200 København K

Fra: Anders Thomsen [athomsen@microsoft.com]
Sendt: 25. juni 2012 15:46
Til: Justitsministeriet
Emne: J.nr. 2012-3756-0005 - svar på høring
Vedhæftede filer: Microsoft position on EU Privacy Regulation - February 2012.pdf

Microsoft Danmark svarer hermed på Justitsministeriets høring over "Forslag til en generel forordning om databeskyttelse" af 15. maj.

Microsoft var blandt de første til at sætte privacy på dagsordenen. De tre principper ansvarlighed, gennemsigtighed og valgmuligheder er fundamentet for Microsofts tilgang til privacy. Vi arbejder for ansvarligt at styre og beskytte de data vi opbevarer, at være åbne om vores privacy aktiviteter og at tilbyde meningsfulde privacy valgmuligheder. Microsoft arbejder for globale policy rammer som placerer hovedbyrden for ansvarlig brug af personlig data hos virksomheder fremfor forbrugere.

Microsoft Danmark kan bakke op om den foreløbige danske holdning med fokus på at finde den rette balance mellem databeskyttelse og innovation samt mellem merværdi og omkostninger. Forslaget til forordning vil være afgørende for, om EU kan gribe alle de muligheder for innovation, effektiviseringer og nye services som ny teknologi giver mulighed for.

Derudover henviser Microsoft Danmark til høringssvaret fra DI ITEK samt vedhæftede notat om forslaget (på engelsk) udarbejdet af Microsoft til brug i den europæiske debat om forordningsforslaget.

Best regards/Med venlig hilsen
Anders Thomsen
Government Affairs manager/ Direktør for politik og strategi
Microsoft Danmark
Tuborg Boulevard 12
DK-2900 Hellerup
Phone: +45 45678164
Mobile: +45 51578315
E-mail: athomsen@microsoft.com

Microsoft, February 2012

The EU's Proposed Data Protection Regulation: Microsoft's Position

On 25 January 2012, the European Commission announced a proposed *General Data Protection Regulation*. The Commission's proposal introduces sweeping reforms designed to modernise Europe's 17-year-old data protection regime.

Microsoft welcomes steps to strengthen and harmonise the data protection regime. Our company's greatest asset is customer trust and our technologies are developed with data protection in mind. Our priority is to protect personal data in an age where we support ubiquitous connectivity, pervasive online business and social networking, and flows and storage of information all over the world on all kinds of computers and devices.

Our efforts have led us to conclude that enterprises, including Microsoft, have a critical role to play in protecting privacy – a role that includes embedding privacy protection into products and services early in and throughout the design cycle, and being transparent about how we collect and use data. We place particular value on transparency, because it enables our customers to make informed choices about how their data is used. With this in mind, we have invested heavily to provide clear and easy-to-understand guidance about how we gather, store, manage and secure information. Microsoft's Office 365 Trust Center[1] is a concrete example of how we put our privacy principles into practice. The Office 365 Trust Center provides transparency about how we promote privacy and security, what international standards we adhere to, and how data flows in our services, among other matters.

Of course, industry efforts alone are inadequate to ensure the privacy and security of personal data. A regulatory environment that promotes transparent and responsible practices is also essential. It is clear, however, that the dramatic technological changes of the past decade have tested Europe's existing data protection framework (Directive 95/46/EC). While the explosive growth of the internet has brought us tremendous social and economic benefits, internet technologies have also fundamentally expanded how, where and by whom data is collected, transmitted and used.

The rapid growth of cloud computing is a prime example. Attracted by the significant cost savings and flexibility of cloud services, individuals, businesses and governments are storing and sharing unprecedented amounts of information online, leading to a significant increase in the quantity and types of data collected and processed by third parties. Cloud technologies offer great promise for Europe, with estimates indicating that the cloud will create a million new jobs and several hundred thousand new small- and medium-sized enterprises, and drive down the cost of ICT for the public and private sectors.[2] But these and many other web-enabled benefits

[1] http://www.microsoft.com/en-us/office365/trust-center.aspx.

[2] *See* F. Etro, *The Economics of Cloud Computing* (March 2011), available at http://www.intertic.org/Policy%20Papers/JManEc.pdf.

will only be realised if users have confidence that their personal data and the data they process for others are safe in the cloud.

The challenge before us is thus how to protect Europeans' privacy while also encouraging innovation and facilitating the productivity and cost-efficiency offered by new computing paradigms like the cloud. The Regulation adds a number of important measures that will help to achieve these goals, including requirements that companies design technologies with privacy in mind, be transparent about their processing activities, and remain responsible for how they use personal data. The proposal also helpfully addresses inconsistent rules and interpretations across the 27 EU Member States, reduces the administrative paperwork for companies, and improves mechanisms to transfer data safely outside of the EU.

Other proposals – particularly those relating to online technologies – need refining to ensure that the protections they offer are both strong *and* workable. For example, the Regulation in some places dictates not only *what* obligations apply, but also *how* those obligations should be implemented – moving the Commission beyond creating regulation to support privacy and into designing technology and business processes. Overly prescriptive approaches in areas like a "right to be forgotten," data portability, and consent do not always reflect how the internet is technically structured today, what consumers want and need, or how technology is likely to evolve tomorrow. Obligations that cannot be properly implemented due to technical hurdles, or that frustrate data subjects, or that become obsolete when technology changes, will be of little lasting value.

The next generation of privacy regulation in the EU ultimately needs to achieve two ends: it must both provide transparency and robust protection to data subjects as well as allow organisations to innovate while holding them accountable to achieving an appropriate level of data protection. Achieving both of these goals will enable Europeans to benefit from online services offerings and to compete globally by innovating to create their own services. A regulatory environment that achieves these ends is particularly important for small- and medium-sized European businesses to innovate successfully, leading to job and wealth creation. This is a serious challenge, but also a tremendous opportunity for responsible companies – and indeed for all of us concerned with the protection of data.

In the hope of strengthening the Regulation, we offer below some initial comments:

- **Main establishment.** Under current EU law, companies with a presence across Europe often need to address multiple, and sometimes divergent, national data protection regimes. The Regulation helpfully meets this challenge by proposing a single law for Europe and by setting a goal that companies processing data in the EU will be subject to a single supervisory authority based on their country of "main establishment."

  Yet the Regulation defines "main establishment" in a way that may add to confusion rather than reduce it. For example, to determine a processor's main establishment, the Regulation looks to the place of "central administration" – a term that is undefined and in practice may have *no relation* to the market where data is in fact processed. The Regulation uses a

somewhat more sensible test for controllers, based on where "main decisions" about processing are taken in the Union – but then introduces an unclear and circular test relating to "main processing activities" in the context of an establishment. The result may be that multiple data protection authorities claim jurisdiction over organisations, especially organisations that act as both processors and controllers in multiple Member States.

We would recommend a common-sense, simple approach that (i) applies across the board to controllers *and* processors alike, and (ii) defines "main establishment" by reference to the physical location of an entity's primary data centre (i.e., where the controller/processor has its physical infrastructure for processing data). *This approach ensures that there is a close link between the market where data is processed and the DPA supervising that processing.* As a fall-back, for those companies that lack processing facilities in the EU (for example, for firms that outsource their processing), we support a definition based on the Regulation's existing test for controllers, i.e., that gives the Member State where key decisions about processing are made authority over that processing.

- **The role of data processors.** A robust data protection regime needs to delineate the responsibilities of the different parties involved in processing information clearly and ensure that the parties bear burdens that are appropriate to their role in the business ecosystem. In this regard, the Regulation correctly continues to place the onus for compliance primarily on data controllers.

  The Regulation also increases the obligations on processors, however. While increased obligations in some areas may be warranted, these new responsibilities should reflect both the complex contractual environment in which processors operate and the limited control they often exercise over data they are processing. For example, the Regulation requires that processors grant supervisory authorities access to data in certain circumstances – apparently regardless of any competing contractual obligations. The liability of processors also increases under the new regime – again, despite the fact that the processor may already independent contractual liability to the controller. These and other aspects of the balance in responsibilities between controllers and processors should be carefully considered in light of contractual obligations already imposed on processors, in order to avoid potential contradictions stemming from overlapping responsibilities.

  The Regulation could also be clearer in terms of the dividing line between processors and controllers. With the evolution of technologies like cloud computing, the distinction between processors and controllers can sometimes blur. While the Regulation does seek to clarify these roles, further guidance and precision in this regard would be useful. Because the Regulation applies different tests and obligations to controllers and to processors, it will be essential for enterprises to understand clearly when they are controllers and when they are processors. For example, as noted above, the Regulation proposes different tests for "main establishment" for controllers and processors; if an enterprise is not clear on the role it is playing, it cannot determine which test applies or identify its supervising DPA.

- **Right to be forgotten**. Under Directive 95/46, data controllers have the obligation to erase personal data at the direction of the data subject in certain scenarios. The Regulation builds on this principle by giving individuals a "right to be forgotten" (RTBF). As conceived in the Regulation, the RTBF would not only require companies in certain circumstances to erase personal data upon a request from the data subject, but also, where that data has been made public, the company involved would be required to inform *any third parties* processing that data about the request to erase copies of or links to that data. The Regulation imposes harsh penalties on controllers that fail to comply.

  The structure of the RTBF does not fully reflect the structure of the internet, however. Digital data today is often quickly replicated across the web on systems and servers across the globe with or without any formal technical or contractual relationships between different parts of the online ecosystem. For example, many search engines and content aggregators use publicly available internet information to catalogue and build large caches of data without any explicit contractual agreement with the primary publisher of the information. These caches are what make it possible for individuals to find data quickly on the internet when they do an Internet search. However, as a result, it can be difficult if not impossible to "remove all tracks." By requiring that controllers notify any and all third parties, the RTBF provision seems to envisage that companies *can* oversee the entirety of the World Wide Web and control the information on it – an obligation that is directly at odds with the open architecture of the internet. Indeed, European law (in the E-Commerce Directive) already recognises that it would be unreasonable to ask companies to monitor the internet and makes clear that companies should not be required to do so.

  To be workable, any interpretation of the RTBF must not obligate companies to do that which is technically impossible. Accordingly, the Regulation should limit the RTBF to that data *retained by and under the control* of the controller and *reasonably accessible* in the ordinary course of business. At the same time, the RTBF should extend only to a user's own data (i.e., data that a user inputs directly) and not to data generated in the operation of the service (for example, error messages or uptime statistics). And for user convenience, service providers should also be permitted to retain data for a limited period in order to re-enable users where users expressly request this.

- **Data portability**. With the increasing use of online services, social networks and cloud technologies to hold all sorts of personal data, it has become increasingly important that users are able to take their data with them when they leave a service. The Regulation seeks to ensure this by proposing that individuals be able to "port" their data. But the Regulation goes beyond this, and requires that the data be returned to users in a way that allows for a direct transfer to other services. The Regulation also gives the Commission the power to impose technical standards governing the format in which data is to be returned.

  Microsoft absolutely supports giving individuals more control over their data – increased data mobility is not only good for users, it is also good for business and the overall ecosystem. But the Regulation should recognise the technical reality that the ability to

export data does not necessarily mean that such data can be used "as is" in other services. Companies use a wide range of mechanisms to enable the export of data – among them industry standard formats, import/export functions and APIs permitting others to connect to the data directly – depending on the technology, service and functionalities involved. And new mechanisms are invented every day. As a result, the successful transfer of data from one service to another is not a simple proposition – and mandating a single format for data transfer will require technology providers to change other aspects of their products and services which may result in less functionality, less diversity and a worse overall user experience.

We propose a solution that permits users to port the data they had originally created, but allows industry to decide on formats and technical details of returning user data back to users, based on a variety of technical and commercial factors – including an emphasis on ease of use and the prevalence of a particular format and method.

- **Certifications.** The Regulation helpfully promises to promote certifications and other mechanisms to encourage organisations to demonstrate their security and privacy commitments. Microsoft welcomes such efforts and has been at the forefront of pursuing many industry leading certifications. However, Microsoft would like to encourage the Regulation to support international certifications, including EU-adopted international certifications, instead of sector-specific or regional certification programs, which can lead to fragmentation of standards in privacy and data security. Industry with other relevant stakeholders should be deeply involved in developing the certifications so their expertise is incorporated, with oversight and help from the Commission.

- **Profiling.** The use of the internet and the proliferation of connected devices generate unprecedented levels of data – which can sometimes be used to build profiles. Profiling itself is merely a technical process that helps identify patterns across large quantities of data, and in doing so allows information to be collected and organised in meaningful ways. As such, there is nothing inherently wrong with profiling. Indeed, profiles are frequently used to satisfy consumer demands for technologies and services that remember their preferences, such as their native language or home country, or that are customised in other ways.

  Of course, as with any business process, automated profiles can also be used to achieve less desirable outcomes, such as discriminating against individuals on the basis of their health. To ensure that user data is not used to achieve goals that are contrary to EU citizens' interests, it makes sense to regulate the use of profiles for harmful purposes. However, such rules should not restrict the building of profiles for *all purposes* – including beneficial purposes that are intended to respond to legitimate consumer demands.

  The robust protection of data subjects will be better served if the Regulation focuses on how profiles are used, instead of on the mechanisms used to create profiles. The Regulation should be amended to make clear that profiles can continue to be used for beneficial purposes such as providing customised internet experiences to users.

- **Data breaches.** Data breaches are a recurring challenge to individual privacy. A breach notice obligation is thus key to ensuring that data protection authorities (DPAs) and data subjects are informed and can take appropriate measures where serious breaches threaten significant harm.

  As crafted, however, there is a real risk that rather than promoting good practices, the breach notice provisions in the Regulation will discourage them. For example, the Regulation does not include any threshold test for when DPAs must be notified about a breach. Instead, the Regulation requires *all* controllers in *all* sectors to notify DPAs about *all* breaches, regardless of their gravity, within 24 hours; failure to comply exposes a controller to penalties up to 2% of worldwide turnover, even where that failure is simply the result of negligence.

  Under this regime, DPAs may quickly find themselves overwhelmed by notifications, impairing their ability to effectively tackle the truly serious breaches – a problem that will be compounded by the 24-hour deadline, which will lead controllers to notify suspected breaches even in cases where further investigation would have demonstrated there was in fact no breach. And while the Regulation does include a threshold for notifying data subjects (i.e., when a breach is likely to cause an "adverse effect"), the threshold is so low that it means data subjects will likely receive constant notifications – inducing "notice fatigue" and leading consumers to ignore breach notices. Excessive notices may also lead to an unreasonable level of fear among European internet users, which may negatively affect the use of internet-based technologies.

  To ensure the regime is effective, controllers should be required to notify data subjects and/or regulators of a breach only when there is *significant risk of serious harm* to the data subject. Criteria to be considered in making this assessment could include the type of data involved and its sensitivity, the nature of the breach, and the type of harm threatened by the breach. Also, consistent with the breach rules in the 2009 additions to the e-Privacy Directive (2009/136), companies should be required to notify DPAs "without undue delay" rather than within a 24-hour window. And severe penalties for non-compliance should be reserved for those controllers who wilfully and repeatedly fail to notify.

- **Consent.** The Regulation permits controllers to process personal data where the data subject has consented to the processing. To ensure that this consent is meaningful, the Regulation includes a number of important safeguards, among them requirements that consent be freely given and informed, and that companies clearly distinguish requests for consent when those requests are part of broader communications with customers. But in addition to these safeguards, the Regulation also prescribes that consent must be given in one way – i.e., "explicitly," and by either a "statement" or "clear affirmative action by the subject" – no matter the context in which consent is obtained or the data is used.

  As drafted, the need for consent to be explicit could be read to require that controllers operating online force users to affirmatively "opt in" to the use of their data. We believe that this "one-size-fits-all" approach is too narrow. There is currently a wide range of

mechanisms that effectively enable users to control and consent to collection and use of their information depending on the circumstances involved – including some opt-out technologies that provide stronger protection for consumer privacy than some opt-in mechanisms. For example, an opt-out mechanism that provides complete information on how personal data will be used is more protective of consumer privacy than an opt-in mechanism that does not provide complete information. By preferring one mechanism over others, the Regulation diminishes the incentives to develop different and potentially better privacy protecting solutions.

Equally important, by requiring users to opt in to every use of their data, the Regulation will potentially require internet users to opt in dozens of times, if not more, during a single web surfing session or mobile internet use. Yet consumers demand internet services that are fast, easy-to-use and efficient. Onerous and static opt-in mechanisms instituted by controllers anxious to be in unambiguous compliance with an ambiguous requirement will frustrate many users – and ultimately may lead users to opt in as a matter of routine, even in cases where their privacy would be better served by opting out.

Companies relying on consent to process data *should* be required to ensure that consent is informed and meaningful – and this the Regulation does. But the Regulation should also permit innovators to use different mechanisms to obtain consent that reflect how and in what contexts consent is obtained and data will be used.

The Regulation, like the 95/46 Directive, also permits some processing of personal data even when consent is not obtained (for example, under the legitimate interests exception). We welcome this as in some cases consent places too high a burden on the data subject to understand all uses of their information in an ever increasing complex arena of data flows. As with the comments above on profiling, the Regulation should carefully view what uses of data are appropriate and may be permitted even where express consent is not obtained.

- **Responsibility.** Drawing from the international concept of "accountability," the Regulation will require controllers and processors to be "responsible" for how they handle data. For example, the Regulation requires organisations to appoint a data protection officer responsible for compliance. Privacy impact assessments (PIAs) are another important part of being a responsible data steward, and the Regulation usefully clarifies that companies should carry out PIAs when processing operations "present specific risks to the rights and freedoms of data subjects."

  These reforms, and others like them, will help keep data safe. But we believe that certain changes will help to make these responsibility obligations even more robust. For example, with regard to PIAs, the Regulation stipulates that controllers and processors must *seek the views of data subjects* when conducting PIAs, and consult with supervisory authorities prior to processing the data in those cases where a PIA "is likely to present a high degree of specific risks." In this scenario, national authorities and data subjects could soon find themselves overwhelmed by PIAs (Microsoft alone undertakes *over 2000 PIAs each year*). Moreover, mandating the disclosure of PIAs could change the nature of privacy assessments

by making companies less candid in their evaluations; mandated disclosure could also *undermine* the protection of data by creating risks to the confidentiality of information. We thus recommend that these requirements be eliminated. At a minimum, we would welcome greater clarity as to *exactly* when these rules apply to processors; such clarity is essential, particularly because the Regulation subjects even negligent non-compliance to harsh penalties.

In addition, more broadly, we believe it is important to motivate companies to be responsible by providing clear benefits for doing so. The new regime should encourage good practices by rewarding organisations that demonstrate responsibility and adopt and validate particularly rigorous data protection programs. One way to do this would be to allow organisations that have demonstrated themselves to be responsible – for example by implementing global data protection standards such as ISO 27001 or 27002 – to transfer data across international borders with reduced administrative requirements.

- **Data protection by design and default.** The Regulation also proposes an industry-wide "privacy by design" (PbD) obligation – another integral part of responsibility. Microsoft believes strongly in PbD. Microsoft works hard to ensure that we engineer privacy into our products and online services at the outset of development, review all products and services to identify privacy issues at an early stage; help product groups follow Microsoft privacy policies and standards, and encourage the continued consideration of privacy and data security throughout the product lifecycle.

  We strongly support a PbD obligation. We also welcome the fact that rather than dictate in prescriptive terms how PbD is to be implemented, the Regulation instead dictates the *outcome* that enterprises must be achieve – leaving technology providers free to innovate so long as their innovations protect privacy. Consistent with this approach, we also recommend that express language be added to the Regulation making clear that when the Commission adopts delegated and implementing acts in the area of PbD, this legislation should not take the form of design mandates or technology preferences. Mandates and preferences only serve to impede the development of new technologies, with no guarantee of stronger privacy protections.

  Importantly, in addition to PbD, the Regulation also includes a new and vague obligation requiring controllers to implement mechanisms to ensure that *by default* they process only data that are necessary for each specific purpose of the processing. The intention here may be well founded – we recognise that default settings play an important role in protecting privacy. But, in practice, it is unclear what this obligation entails. This lack of clarity creates uncertainty and, combined with the possibility of the Commission setting "technical standards" in this area, could have unintended negative consequences, such as impairing innovation, limiting functionality and creating user frustration. We would recommend instead that, as part of PbD, the Regulation encourage innovators to assess the full universe of potential privacy risks and make appropriate decisions about privacy designs and settings.

- **Enforcement.** Robust rules on the books are a key element of a strong data protection regime. But effective enforcement of those rules is equally important to ensure that companies take their responsibilities seriously. Supervisory authorities should be granted the power to impose meaningful sanctions for flagrant or repeated violations that threaten real harm to the individuals affected.

  Consistent with this view, the Regulation includes strong sanctions for violations. But less helpfully, the Regulation again takes a "one-size-fits-all" approach, and could be read to apply the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely accidental. This means that a company that inadvertently fails to use a specific electronic format when giving a customer access to his information could face the same penalty as a company that repeatedly and intentionally collects and processes data about individuals without informing those individuals about its activities.

  At the same time, the Regulation also could be read to restrict the discretion of DPAs by requiring them to impose penalties. Specifically, the Regulation might require that where a violation has occurred, DPAs *must* impose a fine – even where that violation may not, in the eyes of the responsible authority, merit one. Any automatic assessment of penalties will inhibit companies from self-reporting, reducing overall transparency, security and privacy. This approach may have a particularly chilling effect on small- and medium-sized European internet-based businesses.

  To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for *truly bad actors*. This requires that DPAs be given the authority to impose sanctions only where truly warranted. It also requires that unintended missteps be subject to separate and lesser penalties, and that there are clearly-established "aggravating" and "mitigating" factors that guide when a penalty should be at the high end of the range and when a penalty should be at the low end. While the Regulation identifies some factors that DPAs should consider in assessing fines, the list is not comprehensive. Additional factors could include, for example, the sorts of measures the company involved took to avoid the breach, whether the company was genuinely uncertain about whether the activity constituted a breach of relevant obligations, and if the organisation took steps to remedy the breach immediately upon becoming aware of it.

- **Secondary rulemaking.** Among the most important reforms, the Regulation introduces a range of measures to better harmonise data protection rules across the 27 Member States. These measures include, for example, a welcome proposal that would subject a controller to a single supervisory authority even when that controller's operations span Europe.

  More worrying, however, the Regulation would also give the Commission substantial authority to adopt delegated and implementing acts in virtually every area covered by the proposal. These acts could include technical standards, design requirements, criteria for technical measures and other conditions defining how obligations are to be implemented. Some of these acts may also be sector specific.

The Commission's ability to propose secondary legislation in a wide number of areas threatens to complicate, rather than simplify, data protection. If new rules are regularly adopted, it effectively means that the benchmarks for data protection are always changing and it becomes virtually impossible for enterprises ever to achieve compliance. Moreover, if the Commission chooses to adopt highly prescriptive measures or dictate specific technology outcomes via delegated and implementing acts, this could potentially hinder innovation in privacy protection.

Rather than seeking to promote greater harmonisation through the adoption of secondary rules, we believe it would be better to rely on other harmonising mechanisms already in the Regulation, such as the single supervisory authority, the European Data Protection Board, and mutual assistance and joint operations among national regulators. At a minimum, the Regulation should make clear that any secondary rules do not take the form of design mandates or preferences for particular technology solutions.

Til
Justitsministeriet
Slotsholmsgade 10
1216 København K
Att.: Christian Wiese Svanberg - sags nr. 2012-3756-0005
jm@jm.dk

Torsdag den 21. juni 2012

ISOBRO's høringssvar til udkast til EU forordning om beskyttelse af personlige data

ISOBRO og ISOBRO's medlemmer lægger stor vægt på beskyttelse af personlige data og har forståelse for hensigten med mange af forordningens artikler. Men hensigterne må ikke udmøntes på en måde, som i urimelig grad hæmmer den samfundsudviklende frivillige, forebyggende, almennyttige og humanitære og udviklende indsats. Overordnet har ISOBRO følgende bekymringer i forbindelse med reglerne.

1. ISOBRO vurderer, at forordningen i sin nuværende udformning risikerer at gøre administrationen unødigt tung for indsamlingsorganisationerne og bringer de administrative omkostninger i vejret. Det er i konflikt med ønsket om, at så stor en del af de indsamlede midler går til "det gode formål"

2. I udkastet til forordning reguleres alle ens på de fleste områder. Men i virkelighedens verden er der en himmel vid forskel på store multinationale foretagender og små frivillige, forebyggende, humanitære og udviklende organisationer, hvor mange aktiviteter drives for indsamlede midler. Det bør reflekteres i flere af forordningens artikler

3. ISOBRO ser kritisk på, at mange af bestemmelserne er ganske uklare, og at det i alt for høj grad overlades til EU kommissionen at fastsætte regler og retningslinjer. Det skaber usikkerhed for alle, og især for frivillige og almennyttige organisationer, da deres vilkår ikke står højt på EU kommissionens dagsorden

4. ISOBRO ser med bekymring på den uindskrænkede bevisbyrde og de meget store bødestørrelser, der kan være ødelæggende for en organisation med store forpligtelser og lille kapital.

Derudover har ISOBRO en række supplerende og mere konkrete bemærkninger til EU forordningen:

a. Aftaler om medlemskab, støttemedlemsskaber og donationer med tilhørende betalingsaftaler indgås overvejende mundtligt. ISOBRO ser positivt på, at der også fremover skal gives eksplicit samtykke i forbindelse med f.eks. oprettelsen af en betalingsaftale. Men det er helt afgørende, at indsamlingsorganisationerne fortsat kan indhente dette samtykke mundtligt,

hvorefter organisationerne umiddelbart herefter opsummerer aftalen og det afgivne samtykke skriftligt i et velkomstbrev hvorfor ingen er i tvivl om aftalen indhold. Muligheden for mundtligt samtykke bør fremgå ikke bare implicit men eksplicit af forordningens artikel 7.

b. Det er ligeledes afgørende, at dokumentationen af det mundtlige samtykke kan håndteres fleksibelt uden at påføre organisationerne store merudgifter - ikke mindst fordi indsamlingsorganisationerne altid annullerer et medlemskab eller en donoraftale, hvis nogen sår tvivl om aftalen eller fortryder - også selv om der på en båndet optagelse er dokumentation for, at der er givet eksplicit samtykke.

c. Forordningen stiller en række krav til bl.a. indsamlingsorganisationerne om at formulere politikker for beskyttelse af de personlige data, beskrive alle processer med behandling af personlige data og udarbejde instrukser til medarbejderne samt sikre, at alle processer er i overensstemmelse med forordningen, jf. artikel 11, 22 og 28. Det er vigtigt, at politikker, procedurer, instrukser og dokumentation kan holdes på et rimeligt overordnet niveau, så indsamlingsorganisationerne ikke får presset de administrative omkostninger unødigt i vejret, fordi kravene er unødigt bureaukratiske eller for ensidigt tilpasset virkeligheden blandt store kommercielle aktører.

d. Udvidelsen af informationspligten i forbindelse med indgåelse af aftaler, jf. artikel 14, volder ikke problemer, hvis det kan accepteres, at de mange informationer, herunder informationer om opbevaringsperiode og klageret mv. f.eks. kan gives på bagsiden af velkomstbrevet, således at forsiden kan reserveres til sagen, taknemmeligheden og opbygning af relationer.

e. Det er afgørende, at en velbegrundet ændring i en administrativ praksis kan gøres gældende over for alle medlemmer – også selvom den afviger fra det oplyste i forbindelse med hvervningen. Det vil være en uoverskuelig byrde for indsamlingsorganisationerne at skulle administrere medlemsoplysninger forskelligt afhængigt af indmeldelsestidspunkt. Massesletning 2 – 4 gange årligt er den mest økonomieffektive måde for indsamlingsorganisationerne at håndtere udløb af opbevaringsperiode.

f. Retten til at forsvinde, jf. artikel 17, bør give mulighed for, at organisationerne ved en total sletning trods alt kan opbevare den oplysning, at den pågældende borger ikke ønsker at blive kontaktet. Derved undgår begge parter nyttesløse samtaler.

g. Artikel 7.3. kan læses således, at det bliver ulovligt at bruge data fra den dato, hvor et samtykke er trukket tilbage. Det er for restriktivt, da det kan tage 1-2 uger at få informationen frem til alle brugere af de pågældende data. Forbuddet bør først træde i kraft efter informationsperiodens udløb.

h. I dag får indsamlingsorganisationerne kun få henvendelser om indsigt i egne data, som håndteres telefonisk. I en håndtering via mail eller automatisk elektronisk svar kan det være sværere at verificere, at den, man kommunikerer med, er den, vedkommende giver sig ud

for, jf. artikel 12. ISOBRO håber, at den telefoniske håndtering fortsat vil være en mulighed for indsamlingsorganisationer.

i. ISOBRO ser positivt på forslaget om, at alle instrukser til bureauer skal foreligge skriftligt, jf. artikel 26. Også her skal der imidlertid være grænser for detaljeringsgrad.

j. Indsamlingsorganisationerne indgår i et kompleks samspil med bureauer og dataoperatører, der f.eks. indsamler eller har adgang til personlige data, som er nødvendige for at løse specifikke opgaver for indsamlingsorganisationerne. Organisationerne indsamler selv cpr numre og kontonumre, som skal bruges af banken for at oprette de aftalte betalingsordninger. Derudover modtages der dataudtræk fra CPR registret. Der skal være sikkerhed for, at bortfaldet af 3. parts legitime rettigheder i artikel 6 ikke skaber huller, hvad angår legitimiteten i dette komplekse samspil.

k. Reglerne om indberetning af brud på databehandlingsprocedurer bør udformes, så organisationerne ikke skal bruge tid og kræfter på at indberette små afvigelser, for så vidt der kun er minimal risiko for misbrug eller andre gener for de berørte mennesker, jf. artikel 31.

l. ISOBRO noterer, at det bliver vanskeligere at komme i kontakt med potentielle medlemmer og donorer gennem små konkurrencer og undersøgelser pga. kravet om eksplicit samtykke i adskilt miljø.

En let og uhindret kontakt med borgere, der er interesserede i at bakke op bag den forebyggende, almennyttige, humanitære og udviklende indsats mv. er afgørende for indsamlingsorganisationerne. Derfor er det af stor betydning, at forordningen ikke fører til begrænsninger i brugen af de åbne telefonbøger, dataudtræk fra CPR registret eller i retten til at vende tilbage til en kunde eller et medlem med nye tilbud. Noget som i dag er sikret i anden lovgivning. Derfor efterlyses der en grundig analyse af den foreslåede forordnings eventuelle påvirkning af EU direktiver og dansk lovgivning udover dem, der direkte vedrører persondatabehandling.

Afslutningsvist vil ISOBRO meget gerne bidrage til et branchekodeks om håndtering af personlige data, jf. artikel 38. Det ligger i god forlængelse af ISOBRO's arbejde med etiske retningslinjer på andre områder.

Sekretariatsleder Mette Holm kan på 38 38 46 80 kontaktes for uddybende bemærkninger.

Med venlig hilsen
ISOBRO

Robert Hinnerskov
Generalsekretær

Fra: Mette Holm - ISOBRO [mailto:mh@isobro.dk]
Sendt: 28. juni 2012 11:30
Til: 'jm@jm.dk'
Cc: 'Robert Hinnerskov'; 'Denise Dawes, European Fundraising Association'; 'Günther Lutschinger'; 'Gosse Bosma'; 'ly@isobro.dk'; 'vibeke.andersen@metodekompagniet.dk'
Emne: Høringssvar - journal nr. 2012-3756-0005

Til
Justitsministeriet

Hermed fremsendes The European Fundraising Associations høringssvar til udkast til EU forordning om beskyttelse af personlige data.

Med venlig hilsen / best wishes
Mette Holm
Sekretariatschef
ISOBRO
Peter Bangs Vej 1D, 2000 Frederiksberg
mh@isobro.dk http://www.isobro.dk
☎ 0045 38 38 46 83 ▪ 0045 26 79 20 26

European Fundraising Association

Comments from the European Fundraising Association on the proposed EU Regulation on the protection of individuals with regard to processing of personal data

The European Fundraising Association acknowledges the importance of protecting personal data. The proposed EU regulation, however, makes administration procedures unnecessarily burdensome for small fundraising organisations, and it will constrain charity fundraising. The European Fundraising Association urges the EU to modify the proposed regulation to ensure that it does not hinder invaluable charitable and non-profit humanitarian, social and health activities carried out by the third sector.

Furthermore, many of the proposed articles are vague and the Regulation contains a vast number of delegated acts and implementing acts. Delegated acts, in particular, grant the Commission considerable leeway in filling in the data protect framework. It creates undue uncertainty, especially among fundraising organisations, as their working conditions do not have high priority on the EU Commission's agenda.

The intent of the Commission is to build a stronger and more coherent data protection framework in the EU. But a more coherent framework does not mean that everybody should be treated in exactly the same way. It as a huge problem, that the regulation does not reflect the tremendous difference between small partly volunteer-based charitable organisations and large multinational enterprises.

The proposed regulation will considerably change the working conditions for all fundraising organisations in Europe, and in some countries the changes will be extensive, depending on the national implementation of the present Directive 95/46/EC. All over Europe the proposed regulation will require extra administrative efforts and investments in new or modified computer systems. Elaborating policies for the protection of personal data, the descriptions of all the procedures to be followed in the processing of personal data, detailed written instructions for employees and documentation to ensure that all procedures are in accordance with the regulation will also result in higher administrative cost. New investments and higher administrative costs contradict the overall objective of ensuring that as much of the fundraised money as possible be used for the charitable causes it was given for.

In addition, the European Fundraising Association is concerned about the unrestricted burden of proof and the suggestion of huge fines, which can be devastating for a charitable organisation with substantial commitments and limited funds.

The European Fundraising Association strongly urges that the regulation reflects the reality of fundraising organisations, in order to ensure that fundraising organisations' administrative costs will not increase due to regulations being unnecessarily bureaucratic or unilaterally adapted to the reality of the large commercial companies. We hope the EU will take into consideration that fundraising organisations pursue high ethical standards in their daily practice, and that data breaches are practically non-existent in this field.

It is of vital importance for fundraising organisations using telemarketing that persons can give their affirmative consent, for instance to a direct debit mandate, verbally. This is particularly so in countries where this practice is already allowed, because the organisations immediately send a welcome letter with a summary of the agreement and the affirmative consents, and because the new member or donor can easily stop the agreement and direct debit mandate in case of any objections or second thoughts.

The European Fundraising Association acknowledges the importance of careful information about the use of personal data, including the period of storage and complaint procedures. We are also willing to disclose the source of personal data if asked. However, in daily practice it is very important that the information can be given verbally or on the back of a welcome letter. The front of the welcome letter must be reserved for information about the charitable issue in question and for showing gratitude for the support of the newcomer. This is the most important issue for the relationship. It is also essential that any well-founded changes in practice can be made applicable to all members - even if this entails a deviation from the information given at the moment of entering the agreement and collecting the personal data. Anything else would be an unmanageable burden for fundraising organisations.

Mass deletion a couple of times a year is the most efficient way for fundraising organisations to deal with the expiration of the storage period. We hope this practice will be allowed. The European Fundraising Association also proposes that the right to disappear will allow fundraising organisations not to erase the personal data on suppression lists. Everybody wants to avoid unfruitful conversations.

The regulation can be interpreted in a way that makes it illegal to use data from the moment where consent has been withdrawn. This is too restrictive, as it will take one week or more to inform all users of the data about the withdrawal. Only then should a ban take effect.

Fundraising organisations have a complex collaboration with external telemarketing agencies and data operators, who collect or have access to personal data which is necessary for them in order to solve specific tasks for the fundraising organisations that they work for. Consequently, there must be assurances that the disappearance of a third party's legitimate interests does not create gaps in terms of the legitimacy of this complex interaction.

The specific regulation regarding how to report breaches of data processing procedures should be formulated in such a way that organisations do not have to spend time and effort on reporting small deviations, as long as the risk of abuse or other inconvenience for the people involved is minimal.

Finally, it is essential for fundraising organisation to have easy and unimpeded access to citizens who wish to support charitable efforts. We hope that the regulation in its final version will not constrain this access, neither directly nor by changing EU Directives and national laws, beyond those mentioned and directly related to personal data. We also look forward to an in-depth analysis from the EU Commission of the impact of the proposed regulation for fundraising organisations and the activities of the third sector in Europe.

You are very welcome to contact me for further comments.
Tel: +45 38 38 46 80 / e-mail: mette.holm@efa-net.eu

On behalf of the European Fundraising Association

Mette Holm
President

Kræftens Bekæmpelse

22. juni 2012

Justitsministeriet
Slotsholmsgade 10
1216 København K.
jm@jm

Att. Christian Weise Svanberg
cws@jm.dk

Direktionen

Strandboulevarden 49
2100 København Ø

Tlf +45 3525 7500
Fax +45 3525 7701
www.cancer.dk

UNDER PROTEKTION AF
HENDES MAJESTÆT DRONNINGEN

Høring vedrørende Kommissionens forslag til en generel forordning om databeskyttelse. J.nr. 2012-3756-0005

Kræftens Bekæmpelse har med stor interesse fulgt processen frem til fremsættelsen af det endelige forslag til en generel forordning om databeskyttelse og takker for muligheden for at afgive høringssvar i forbindelse med det fremsatte forslag.

Høringssvaret er inddelt i fem hovedafsnit.

- Første afsnit indeholder indledende bemærkninger til det fremsatte forslag.
- Andet afsnit beskriver forskningsmuligheder og resultater, hvis forsvarlige opretholdelse og videreførelse risikerer at blive sat på spil med det fremsatte forslag.
- Tredje afsnit omhandler Kommissionens ret til at udstede sekundær lovgivning. Kommentar: Kræftens Bekæmpelse opfordrer til, at den nationale indflydelse på persondataretlige bestemmelser på forskningsområdet sikres ved bl.a. at udforme artikel 83 (om behandling af personoplysninger til historiske, statistiske eller videnskabelige formål) på samme måde som artikel 82 (om behandling i forbindelse med ansættelsesforhold).
- Fjerde og femte afsnit indeholder bemærkninger og anbefalinger til konkrete bestemmelser, som har stor betydning for dansk sundhedsvidenskabelig forskning og enten bør bibeholdes eller foreslås ændret.

1. Indledende bemærkninger

Kræftens Bekæmpelse bemærker først og fremmest, at den umiddelbare konsekvens af en generel databeskyttelsesforordning er, at persondataloven falder bort. Kræftens Bekæmpelse er bekymret for, at en harmonisering af EU-retten på databeskyttelsesområdet vil betyde, at de enestående muligheder, Danmark har for at udføre registerbaseret sundhedsforskning, begrænses og udhules.

Det gældende EU-retlige fundament for persondataretten, direktiv 95/46 EF, indeholder væsentlige frihedsgrader for tilpasning til nationale forhold. De af direktivets bestemmelser, som vedrører registerbaseret forskning, er blevet implementeret i forskelligt omfang og forskellige varianter i de enkelte medlemslande.

Gældende dansk lov giver mulighed for en smidig og sikker behandling af personfølsomme data i den registerbaserede sundhedsvidenskabelige forskning. Tilsvarende findes imidlertid kun i få medlemslande uden for Skandinavien. Det betyder, at de skandinaviske lande har en enestående førerposition med hensyn til at kunne udføre denne type forskning på højt kvalitetsniveau.

Kræftens Bekæmpelse finder det positivt, at det endelige udkast, i modsætning til tidligere versioner, indeholder bestemmelser, som på flere områder tager hensyn til registerbaseret folkesundhedsforskning. Det gælder blandt andet bestemmelserne i forordningens artikel 83 vedrørende forskning samt artikel 17 vedrørende "retten til at blive glemt".

Kræftens Bekæmpelse er dog stærkt bekymret over, at den foreslåede reguleringsteknik giver Kommissionen betydelige beføjelser til at udstede sekundær lovgivning på en række centrale områder. Det indebærer usikkerhed og giver anledning til bekymring omkring konsekvenserne af forordningen og dermed registerforskningens fremtidige rammevilkår.

I det tilfælde at regulativet medfører harmonisering i overensstemmelse med gældende lovgivning i Danmark og Norden, vil forskningssamarbejdet i Europa forbedres og øges til gavn for den europæiske befolkning. Modsat vil det medføre dyre, omfattende og komplekse procedurer for registerbaseret forskning, hvis harmoniseringen afspejler gældende regler i størstedelen af det øvrige Europa. I nogle medlemslande kan registerbaserede forskningsprojekter slet ikke gennemføres på nuværende tidspunkt, f.eks. på grund af krav om individuelt samtykke i forbindelse med store befolkningsundersøgelser.

Kræftens Bekæmpelse opfordrer indtrængende til, at der sikres rammer for, at registerbaseret folkesundhedsforskning fremover kan gennemføres på samme høje kvalitetsniveau, som Danmark er internationalt anerkendt for.

2. Forskningsmuligheder og - resultater opnået med den danske model

Danmark har en international førerposition på registerforskningsområdet, hvilket bl.a. skyldes en langvarig og veludbygget indberetning til og tilrettelæggelse af registre. Danmark har verdenskendte registre med værdifulde data om befolkningen, og den danske model for registerkobling og videregivelse af data fra registerforskningsprojekter til sundhedsvidenskabelige forskningsprojekter er enestående.

Som eksempler på sager, der alene har kunnet løses, fordi kortlægning på grundlag af registrene var mulig, kan nævnes

- Eternit/Asbestsagen
- Thulesagen[1]
- Mobiltelefoni og kræft-undersøgelsen[2]
- Evaluering af cancerscreeningsprogrammer baseret på kobling af registre fra screeningsprogrammer, cancerregisteret, Landspatientregisteret, Patologiregisteret, Dødsårsagsregisteret mv.[3]

Eksempler på værdifulde projekter, som rammerne i persondataloven har muliggjort, er

- Glostrup-undersøgelserne, hvor man siden 1964 har fulgt en række kohorter fra de vestlige forstæder til København og kan beskrive livsstilsfaktorer, der har betydning for sundheden
- Østerbroundersøgelsen, der er en befolkningsundersøgelse, som har foregået i flere faser siden 1976
- Undersøgelsen Kost, Kræft og Helbred, som omfatter både en befolkningsundersøgelse og etablering af en biologisk bank i Danmark.

Det er forskning, som man i Danmark har haft mulighed for at gennemføre grundet eksistensen af landsdækkende statistikregistre som Cancerregisteret, Landspatientregisteret og Patologiregisteret. Tilsvarende registre af tilsvarende høje kvalitet eksisterer ikke i samme omfang for andre landes befolkninger.

Udstedelsen af en forordning, som tager sigte på at ensrette den nationale regulering i medlemslandene kan have alvorlige konsekvenser for samfundets nytte af den omfattende dataindsamling, som allerede har fundet sted gennem adskillige årtier. Intentionen bag gennemførte befolkningsundersøgelser udhules, hvis indsamlede data ikke fremover kan anvendes i forskningen. Det vil også have negativ betydning for gennemførelsen af fremtidige befolkningsundersøgelser. Endelig kan en harmonisering have alvorlige konsekvenser for den velfungerende danske praksis for registerkobling, som hidtil er sket med forsvarlig beskyttelse af personfølsomme data, og som har ført til forskningsresultater i verdensklasse.

3. Sekundær lovgivning og registerforskning

Forslaget til et generelt databeskyttelsesregulativ giver Kommissionen betydelige beføjelser til at udstede sekundær lovgivning på en række centrale områder. Anvendelse af delegeret lovgivning skaber usikkerhed om fremtidige muligheder for forskning i folkesundhed, især da der er væsensforskellige traditioner og kulturer i forhold til forskning, registrering og registerkobling i Europa.

---

[1] Juel, Knud (2005) Registerundersøgelse af dødelighed og kræftforekomst blandt Thule-arbejdere, 2005. http://www.si-folkesundhed.dk/upload/thule.pdf

[2] Frei, P (BMJ 2011) Use of mobile phones and risk of brain tumours: update of Danish cohort study.

[3] Scandinavian Journal of Public Health vol. 39 supplementum 7, juli 2011.

Der kan kun gisnes om, hvad sådanne regler konkret vil indeholde, selvom forordningen udgør en ramme. Kræftens Bekæmpelse er bekymret for, om Kommissionen vil udstede retsakter om eksempelvis kryperingsmetoder eller brug af Trusted Third Parties (under f.eks. artikel 23.3), som vil give unødigt besvær og øgede omkostninger. Udbyttet af sådanne tiltag for datasikkerheden er ikke entydig. Videre kan sådanne bestemmelser være direkte hindrende for den forskning, vi kender på befolkningsdata i Norden - en forskning som er værdifuld for hele EU. Eventuel indførelse af krypteringsmodeller, som f.eks. gennemføres i Tyskland, kan i høj grad vanskeliggøre denne forskning.

Videre er det uklart, hvor meget Kommissionen kan påvirkes og vil være lydhør for forskningsfaglige argumenter i forbindelse med udstedelsen af delegeret lovgivning.
Kræftens Bekæmpelse finder, at det bidrager til en alvorlig og foruroligende uklarhed og uigennemsigtighed omkring det persondataretlige grundlag for fremtidig forskning i den danske såvel som europæiske folkesundhed.

Anbefalinger
Kræftens Bekæmpelse anbefaler en ændring af artikel 83 (om behandling af personoplysninger til historiske, statistiske eller videnskabelige forskningsformål), således at den udformes på samme måde som artikel 82 (om ansættelsesforhold), der inden for forordningen og med udgangspunkt i det, der nu er nævnt i stk.1 og 2, giver mulighed for, at medlemslandene selv kan fastsætte regler. Med den nuværende artikel 83 anerkendes det allerede, at behandling af personoplysninger til historiske, statistiske eller videnskabelige formål er et særligt område.

Artikel 83(3) om mulige begrænsninger af registreredes ret til indsigt samt præcisering af rettigheder bør ligeledes indgå, så forordningen også på dette punkt indeholder bestemmelser, der udfyldes nationalt med mulighed for forskellighed. Endelig bør dette gælde overholdelse af/tilpasning til artikel 30 (om behandlingssikkerhed).

De regler, som medlemslandene selv måtte fastsætte, skal muligvis meddeles Kommissionen, men efter Kræftens Bekæmpelses overbevisning, giver dette den bedste mulighed for at fastholde en fornuftig regulering på dette væsentlige, men alligevel for persondatabeskyttelsen også specielle område.

Kræftens Bekæmpelse anbefaler, at der sikres størst mulig gennemsigtighed og inddragelse af fagkompetencer/interessenter på øvrige områder, hvor Kommissionen delegeres beføjelser til at udstede sekundær lovgivning. Sekundær lovgivning bør desuden tage udgangspunkt i og tage hensyn til eksisterende, professionelle guidelines på det pågældende område. Det gælder særligt artiklerne:

- 14 (som fastsætter nærmere bestemmelser om den registeransvarliges underretningspligt over for den registrerede)
- 15 (om den registreredes ret til indsigt i sine personoplysninger)
- 23 (om den registeransvarliges forpligtelser som følge af principperne om indbygget databeskyttelse og databeskyttelse gennem indstillinger)
- 30 (som forpligter den registeransvarlige og registerføreren til at gennemføre passende foranstaltninger, der tager sigte på at garantere behandlingssikkerheden)

- 33 (som indfører forpligtelsen for de registeransvarlige og registerførere til at foretage en konsekvensanalyse vedrørende databeskyttelse, inden de foretager risikobehæftet behandling).

4. Konkrete bestemmelser der bør bibeholdes

Kræftens Bekæmpelse ønsker at gøre opmærksom på, hvor vigtigt det er for fremtidig registerforskning, at de nedenfor berørte områder af forslaget til forordningen bibeholdes. (Dette ikke mindst i det tilfælde, at artikel 83 ikke kan udformes på samme måde som artikel 82.)

Samtykke
Det bærende princip for behandling af personfølsomme data er princippet om informeret samtykke. Det gældende direktiv 95/46 EC undtager registerforskningen fra kravet om samtykke, idet det er praktisk umuligt at indhente samtykke fra hele den population, som er genstand for den givne undersøgelse, herunder samtykke fra afdøde personer.

Det er yderst centralt, at den tilsvarende undtagelse i det foreslåede regulativ artikel 9.2 (g), (h) og (i) om behandling af særlige kategorier af personoplysninger, bibeholdes i et endeligt regulativ.

Behandling af data om helbredsforhold
Bestemmelserne i Artikel 81.1 og 81.2 (om behandling af personoplysninger om helbredsforhold) bør bibeholdes, idet forebyggelse og hensyn til folkesundhed nævnes eksplicit som legitime årsager til behandling af personoplysninger om helbredsforhold.

Retten til at blive glemt
Den foreslåede artikel 17.3 (b) og (c) (der undtager fra retten til at blive glemt og ret til sletning) er central for fremtidig registerforskning. Bestemmelsen vil medvirke til at sikre, at datagrundlaget i registre ikke udhules og bør derfor bibeholdes i et endeligt regulativ.

Formål med behandling af personoplysninger
Artikel 5 (b) (om principper for behandling af personoplysninger) angiver, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål. Det er vigtigt at pointere, at fremtidige formål for forskningen i folkesundhed kan være mangfoldige, umulige at forudsige og dermed også umulige at angive udtrykkeligt i forbindelse med selve dataindsamlingen. Det er vigtigt, at man ved formuleringen "uforenelig med disse formål" tilsigter fuld brug af sundhedsoplysninger i registerbaseret forskning med forskelligt/skiftende formål. Et eksempel her er indsamling af biologiske prøver, der med udvikling af de tekniske analysemuligheder og kobling til andre registre/databaser i fremtiden kan give væsentlige oplysninger til bedre sygdomsbekæmpelse og behandling.

Bestemmelsen i artikel 5 (e) er vigtig at bibeholde, idet den åbner mulighed for at opbevare data til forskningsformål i længere tidsrum, og hvis oplysningerne behandles til forskningsformål.

5. Konkrete bemærkninger og ændringsforslag til øvrige bestemmelser

Kræftens Bekæmpelse har konkrete bemærkninger og ændringsforslag til nedenfor beskrevne områder.

Ret til indsigt
Artikel 15 omhandler den registreredes ret til indsigt i sine personoplysninger. Artikel 13.2 i det gældende direktiv giver medlemslandene mulighed for at begrænse retten til indsigt, hvis oplysningerne alene anvendes til videnskabelig forskning eller statistiske formål.

Samme forhold bør gøre sig gældende i et regulativ.

Vigtigt er det her at bemærke, at forskningsregistre ofte indeholder data, indsamlet fra forskellige kilder, og at data ikke er direkte identificerbare i de data, der gøres til genstand for forskningen. Det vil være uforholdsmæssigt vanskeligt at optrevle data for det enkelte datasubjekt.

Kræftens Bekæmpelse foreslår, at forskningsregistre dog skal oplyse, hvor data indhentes samt en generel beskrivelse af, hvad data anvendes til.

Konsekvensanalyse
Artikel 33 omhandler konsekvensanalyse vedrørende databeskyttelse. Kræftens Bekæmpelse er særligt bekymret for, at denne bestemmelse kan føre til omkostningstunge, tidsmæssigt forsinkende og bureaukratiske foranstaltninger for forskningen. Registerforskningsmiljøet har veludviklede retningslinjer både for datasikkerhed og for etik, som har fungeret gennem en lang årrække er yderst operative og imødekommer forsvarlig beskyttelse af personfølsomme data, såsom helbredsoplysninger.

Kræftens Bekæmpelse finder, at det giver anledning til stor usikkerhed at tillægge Kommissionen beføjelser til at udstede sekundær lovgivning på dette område.

Det Europæiske Databeskyttelsesråd
I artikel 65 oprettes et europæisk databeskyttelsesråd og i artikel 72 fastsættes det, at drøftelserne i rådet er fortrolige.

Kræftens Bekæmpelse finder det uklart, om der med denne model er sikret hensynet til forsvarlig iagttagelse af forskningsmæssige samfundsinteresser i forbindelse med den rolle, et europæisk databeskyttelsesråd er tiltænkt. Kræftens Bekæmpelse vil gerne udtrykke en generel skepsis mod, at Gruppen under artikel 29 nedlægges og erstattes med et Databeskyttelsesråd. Kræftens Bekæmpelse finder, at der bør være indsigt i, hvilke emner der er genstand for drøftelse, hvilke konklusioner Databeskyttelsesrådet drager samt indsigt i, hvilke anbefalinger Databeskyttelsesrådet giver.

Åbenhed og indsigt vil som styringsprincip medvirke til at kvalificere og motivere såvel diskussioner og konklusioner.

Kræftens Bekæmpelse opfordrer på det kraftigste til at sikre rammer for, at registerbaseret folkesundhedsforskning fremover kan gennemføres på samme høje kvalitetsniveau, som Danmark og resten af Norden er internationalt anerkendt for.

Med venlig hilsen

Leif Vestergaard Pedersen
Adm. direktør

Justitsministeriet
jm@jm.dk
j.nr. 2012-3756-
0005.

Sendt pr. e-mail.

JPS
DR Byen

DK-0999 København C
T +45 3520 3643
www.dr.dk

Martin Kyst
D 35203922
E MAKY@dr.dk

12/01289
25. juni 2012

Høring over Forslag til ny generel forordning om databeskyttelse

DR har erfaret, at Justitsministeriet ved brev af 11. maj 2012 har sendt Kommissionens forslag til ny forordning om databeskyttelse (persondataforordningen) i høring. DR vil i den anledning gerne fremkomme med følgende bemærkninger.

DR hilser det generelt velkomment, at der nu søges etableret en opdateret retlig ramme for beskyttelse af personoplysninger inden for EU. De nuværende regler er i vid udstrækning blevet overhalet af den teknologiske og samfundsmæssige udvikling, og der er derfor behov for en mere ajourført regulering.

Efter DRs opfattelse kan der sættes spørgsmålstegn ved, om det rette retlige instrument for den fremtidige regulering skal være en forordning, som uden videre har virkning i alle medlemsstater. Den eksisterende beskyttelse af personoplysninger bygger på direktiv 95/46 af 24. oktober 1995, og er i Danmark gennemført ved lov om behandling af personoplysninger. Reguleringen ved hjælp af et direktiv giver medlemsstaterne en mere fleksibel mulighed for at tilpasse de fællesskabsretlige forpligtelser til danske retstraditioner, og DR vil foretrække, at den fremtidige regulering på dette område også kan finde sted inden for disse mere fleksible rammer. Hvis det imidlertid besluttes at arbejde videre med et forslag til forordning, skal DR opfordre til, at der foretages en betydelig forenkling af de foreslåede regler; det er af afgørende betydning, at der ikke pålægges DR og andre offentlige virksomheder yderligere forpligtelser, som i væsentlig grad vil forøge de administrative byrder, forbundet med administrationen og overholdelsen af regelsættet.

I forhold til DR er en af de helt centrale bestemmelser i forordningsudkastet bestemmelsen i art. 80, hvorefter medlemsstaterne kan fastsætte fritagelser eller undtagelser fra de generelle principper og rettigheder i forordningen. Som eksempel nævnes en undtagelse for behandling af personoplysninger, der finder sted i journalistisk øjemed. Bestemmelsen skal sammenholdes med betragtning nr. 121 i forordningsudkastet, som uddyber forholdet mellem denne undtagelse og de grundlæggende rettigheder om bl.a. beskyttelse af ytringsfriheden. Der er i forordningsudkastet lagt op til en fakultativ adgang for medlemsstaterne til at indføre undtagelser for massemediernes behandling af personoplysninger. Det er afgørende for DR, at der i lighed med persondatadirektivets art. 9 fortsat sikres adgang til at undtage den journalistiske behandling af personoplysninger, eftersom hensynet til ytringsfriheden i dette tilfælde må veje tungere. DR vil derfor opfordre til, at dette i de videre forhandlinger præciseres yderligere, således at massemedierne også i fremtiden alene vil være underlagt de mere lempelige forpligtelser, som følger af lov om massemediers informationsdatabaser.

En af de væsentligste nyskabelser i forordningsudkastet er den såkaldte "ret til at blive glemt"-bestemmelse, jf. art. 17. Bestemmelsen giver den registrerede ret til at kræve, at den registeransvarlige skal slette personoplysninger vedrørende den registrerede. Der er endvidere en forpligtelse for den registeransvarlige til at underrette tredjeparter, som behandler personoplysninger, om at den registrerede ønsker alle links til eller kopier af personoplysningerne slettet. Dette forekommer at være en meget vidtgående forpligtelse, som det i praksis vil være særdeles vanskeligt – endsige umuligt – for den registeransvarlige at efterleve. Dette gælder i særdeleshed, når man tager højde for den spredning af personoplysninger, som finder sted via internettet, søgemaskiner og interaktive sociale medier. Det er på den baggrund DRs opfattelse, at denne forpligtelse bør nedtones, eftersom det i praksis ikke vil være muligt for den registeransvarlige at underrette alle tredjeparter om den ønskede sletning af oplysninger.

I forordningsudkastets art. 6 fastsættes de almindelige betingelser for behandling af personoplysninger, og det følger af art. 6, stk. 1, litra f, at behandlingen af personoplysninger kan finde sted uden samtykke, såfremt behandlingen er nødvendig for at den registeransvarlige kan forfølge en legitim interesse, medmindre den registreredes interesser må gå forud, herunder navnlig hvis den registrerede er et barn. En lignende afvejningsregel findes også i persondatalovens § 6, stk. 1, nr. 7. Såfremt en yderligere behandling ikke er forenelig med det formål, hvortil oplysningerne oprindeligt er indsamlet, skal behandlingen ifølge forslaget til art. 6, stk. 4, have hjemmel i behandlingsreglerne i art. 6, stk. 1, litra a-e. DR finder det uhensigtsmæssigt, at afvejningsreglen ikke også kan anvendes i dette tilfælde og opfordrer på den baggrund til, at art. 6, stk. 4, ændres, således at der henvises til alle behandlingshjemlerne i art. 6, stk. 1, litra a-f.

Forordningsudkastets art. 28 indeholder en bestemmelse om dokumentation. Ifølge bestemmelsen skal den registeransvarlige eller dennes repræsentant opbevare dokumentation for enhver behandling, der gennemføres under denne. Indholdet af dokumentationen er nærmere defineret i art. 28, stk. 2. Undtaget fra dokumentationsforpligtelsen er ifølge art. 28, stk. 4, bl.a. en virksomhed eller organisation, der beskæftiger under 250 personer.

De angivne dokumentationskrav forekommer meget vidtgående og i praksis vanskelige at håndtere for virksomheder og organisationer. Desuden forekommer grænsen på 250 medarbejdere arbitrær. DR finder, at der bør ske en lempelse af dokumentationskravene, således at der ikke bliver skabt nye væsentlige administrative byrder for de enkelte virksomheder og organisationer.

Det følger endvidere af art. 31, at den registeransvarlige er forpligtet til uden unødig forsinkelse og senest inden 24 timer at anmelde et brud på persondatasikkerheden til tilsynsmyndigheden. Det forekommer rimeligt at have en sådan anmeldelsespligt, men den meget korte tidsfrist forekommer unødigt byrdefuld for almindelige virksomheder og organisationer. DR skal derfor opfordre til, at bestemmelsen opblødes, således at anmeldelsespligten lempes i forhold til det foreslåede, fx i form af en længere reaktionsfrist for den registeransvarlige.

Endelig finder DR, at sanktionsniveauet i form af bøder i størrelsesordenen 1.000.000 EURO eller 2 % af en virksomheds årlige globale omsætning er alt for højt; navnlig når man tager de betydelige forpligtelser, som i øvrigt følger af udkastet, i betragtning.

Med venlig hilsen

Martin Kyst
Juridisk konsulent

REGION SJÆLLAND
- vi er til for dig

Justitsministeriet
Civil- og Politiafdelingen,
Slotsholmsgade 10
1216 København K

Dato: 26. juni 2012

Brevid: 1770795

Kvalitet og Udvikling
Alléen 15
4180 Sorø

Tlf.: 70 15 50 00
Dir.tlf. 52 55

kvalitetudvikling
@regionsjaelland.dk
hob@regionsjaelland.dk

www.regionsjaelland.dk

Høringssvar fra RVK Sjælland til Justitsministeriet om forslag til generel forordning om databeskyttelse

Tak for lejligheden for sekretariatet for Den Regionale Videnskabsetiske Komité for Region Sjælland til at kommentere forslaget til generel forordning om databeskyttelse.

En forordning gældende for hele EU vil overordnet være en hensigtsmæssig foranstaltning, da det er fornuftigt at sikre beskyttelse af borgernes personoplysninger på et ensartet niveau i hele EU. Dette vil også smidiggøre håndtering af videregivelse af personoplysninger til sundhedsinstanser i de øvrige EU-lande. Dette bliver stadig mere relevant for den sundhedsvidenskabelige forskning, idet prøver fra forsøg der gennemføres parallelt i flere lande ofte samles med henblik på analyse på ét enkelt laboratorium for at reducere usikkerheden ved analyserne.

Forslaget er dog foreløbig formuleret i meget generelle termer så det er vanskeligt at vurdere konsekvenserne af gennemførelse af forslaget for datasikkerhed, arbejdsgange og økonomi i forbindelse med arbejde med databeskyttelse. Sådanne vurderinger forudsætter en konkretisering/-uddybning af definitioner og krav på bl.a. følgende områder:

- "Passende tekniske og organisatoriske kontroller"
- "Vigtige samfundsinteresser"

Sekretariatet for RVK Sjælland har i øvrigt følgende mere specifikke kommentarer og spørgsmål:

Forslaget til forordning indebærer, at der fremover forventes pålagt drakoniske sanktioner fra administrativt niveau (tilsynsmyndigheden) for at opnå en special- og generalpræventiv effekt – også i tilfælde af uagtsom overtrædelse af forordningens bestemmelser. Det er væsentligt, om der vil foreligge en ankemulighed. Dette understreges af, at de nævnte bødestørrelser reelt kan have en prohibitiv effekt for gennemførelse af sundhedsvidenskabelige forsøg, som komité-systemet på én gang skal føre kontrol med og fremme.

I de indledende betragtninger i kommentar 26 på side 22-23 nævnes medicinsk udstyr og *in vitro*-diagnostik. I den eksisterende danske lovgivning er medicoteknisk udstyr specifikt undtaget fra kravene om log-

ning og adgangskontrol m.v. Det er væsentligt, om denne undtagelse vil bortfalde med den kommende forordning, og i givet fald har det stor økonomisk betydning, om undtagelsen bortfalder for fremtidigt indkøbt udstyr eller også gælder for den eksisterende apparaturpark.

I afsnit 2.5 i Justitsministeriets grund- og nærhedsnotatet afsnit 2.5 angives det bl.a. at: "Som en nyskabelse stiller forslaget også krav om, at den registeransvarlige og registerføreren skal opbevare dokumentation for enhver behandling af personoplysninger, de gennemfører"[notatets side 8, 2. afsnit]. Det er væsentligt, om der her henvises til udkastets artikel 28 eller til anden form for dokumentation, bl.a. fordi kravene i artikel 28 forekommer væsentlig mere begrænsede end i notatet: Notatet giver indtryk af, at man skal dokumentere de enkelte analyser, som gennemføres af data, mens det i artikel 28 opregnes, at man skal dokumentere bl.a. formålene med databehandlingen og kategorierne af data – en dokumentationsbyrde der er væsentlig mindre omfattende end notatet giver indtryk af. Såfremt man skal dokumentere de enkelte analyser, vil det indebære en meget omfattende arbejdsopgave i forbindelse med især registrerforskning men også andre studier, hvor forskerne har behov for at teste mange forskellige kombinationer af data og analyseteknikker for at kunne udvikle ny viden.

Venlig hilsen

Hans Okkels Birk
Konsulent

Realkreditrådet
ASSOCIATION OF
DANISH MORTGAGE BANKS

REALKREDIT
FORENINGEN

Sendt via e-mail: jm@jm.dk

27. juni 2012
S531 - D41229

Justitsministeriet
Slotsholmsgade 10
1216 København K

Att.: fm. Christian Wiese Svanberg

Høring over EU-Kommissionens forslag til nye EU-databeskyttelsesregler - Justitsministeriets j.nr. 2012-3756-0005

Realkreditrådet og Realkreditforeningen (herefter benævnt organisationerne) har med tak modtaget Justitsministeriets brev af 11. maj 2012 vedlagt EU-Kommissionens ovenstående forslag til forordning samt grund- og nærhedsnotat om samme.

Organisationerne er generelt positive over for Kommissionens initiativ til en opdatering af det gældende databeskyttelsesdirektiv (95/46/EF). Direktivet er fra 1995, og vi kan støtte, at EU-lovgivningen på området for persondatabeskyttelse i højere grad kommer til at afspejle den teknologiske udvikling siden da. Samtidig betyder valget af forordning som form, at der sikres en ensartet regulering på området.

Generelt er vi imidlertid bekymrede over, at Kommissionens nye forslag virker meget omfattende og unødigt bureaukratisk. Vi vurderer, at der kan blive tale om mærkbare nye administrative byrder for virksomhederne, der ikke modsvares af tilstrækkelige positive effekter af forslaget.

Udover de administrative omkostninger vil forordningen i sin nuværende form også betyde behov for en betydelig it-udvikling. Det er blandt andet tilfældet i forhold til retten til dataportabilitet, jf. art 18.

I den forbindelse er vi helt enige, når Justitsministeriet i grund- og nærhedsnotatets pkt. 8 angiver, at der er behov for en nærmere vurdering af, "om forslaget skaber den rette balance mellem hensynet til databeskyttelsen og en række andre væsentlige hensyn." Vi finder det ligeledes meget positivt, at Justitsministeriet samme sted skriver, at man fra "dansk side vil arbejde for, at omkostningerne ved forslaget reduceres i forhold til Kommissionens forslag." Det er organisationernes holdning, at det er vigtigt at foretage en grundig undersøgelse af, hvorledes den rette balance opnås. Herunder er det væsentligt at der sikres det rette forhold mellem de administrative byrder og den nytteværdi, der ønskes opnået. Forordningen vurderes ikke at have den rette proportionalitet i sin nuværende udformning.

Da der er tale om en forordning, antager vi, at den nuværende persondatalovgivning viger i sin helhed. Vi har derfor noteret os, at forslaget til forordning vil indebære ophævelse af og/eller væsentlige ændringer i den eksisterende danske persondatalovgivning.

Derudover vil der kunne opstå en lang række afgrænsnings- og fortolkningsvanskeligheder i forhold til gældende dansk lovgivning. F.eks. vurderer organisationerne, at der vil blive tale om en ophævelse af kapitel 9 i Lov om finansiel virksomhed. Dette kapitel indeholder en række bestemmelser om videregivelse af fortrolige oplysninger samt adgang til udveksling af sædvanlige oplysninger. Det er imidlertid uklart, hvilken betydning ophævelsen af disse bestemmelser kan få. Blandt andet gælder der det forhold, at reglerne i FIL omfatter oplysninger om både fysiske og juridiske personer, hvorimod forordningen afgrænses til kun at finde anvendelse på oplysninger om fysiske personer. Det er vores umiddelbare holdning, at der bør iværksættes en grundig analyse af afgrænsninger og afledte effekter i forhold til den eksisterende lovgivning. Før et sådan analysearbejde er afsluttet, er det yderst vanskeligt af fastslå den reelle betydning af indførelsen af forordningen.

Herudover vil vi fremhæve følgende særlige forhold ved forslaget:

Artikel 7 - samtykke

Artikel 7, stk. 1:

Det fremgår af artikel 7, stk. 1, at den registeransvarlige har bevisbyrden i forhold til, at den registrerede har afgivet sit "samtykke til behandlingen af vedkommendes personoplysninger til de angivne formål." Artikel 4, nr. 8, definerer "samtykke" som "enhver frivillig, specifik, informeret og udtrykkelig viljestilkendegivelse baseret på en erklæring eller klar bekræftelse fra den registrerede, hvorved den registrerede indvilliger i, at personoplysninger om vedkommende gøres til genstand for behandling".

I forhold til det gældende direktivs definition (artikel 2, litra h) er "udtrykkeligt" og "baseret på en klar erklæring eller bekræftelse" blevet tilføjet.

I Kommissionens begrundelse for forslaget, pkt. 3.4.1., fremgår, at kriteriet "udtrykkeligt" er "tilføjet for at undgå en forvirrende sidestilling med "utvetydigt" samtykke og for at opnå en fælles og ensartet definition af samtykke, så den registrerede gøres opmærksom på, at og til hvad han eller hun afgiver sit samtykke."

Det efterlader det indtryk, at Kommissionen sigter på at gøre reglerne for afgivelse af samtykke mindre fleksible. Teksten er ikke klar, men en forståelse kunne være, at der f.eks. skal indhentes samtykke hver eneste gang, et realkreditinstitut behandler personoplysninger om en kunde. Hvis dette er tilfældet, vil der være tale om en mærkbar forøgelse af de administrative byrder, som ikke kun er til hinder for virksomhederne, men også for kunderne, som skal afgive væsentligt flere samtykkeerklæringer end nu.

De ændrede krav til samtykke bør kun gælde fremadrettet.

Artikel 7, stk. 4:

Det fremgår af artikel 7, stk. 4, at "Samtykke tilvejebringer ikke et retsgrundlag for behandling, hvis der er en klar skævhed mellem den registrerede og den registeransvarlige."

Det fremgår af præamblens betragtning 34, at skævhed består, hvis der er et afhængighedsforhold mellem den registrerede og den registeransvarlige, og at en sådan afhængighed blandt andet består i ansættelsesforhold.

Vi finder det generelt problematisk, at den almindelige aftalefrihed underlægges specifikke gyldigheds- eller ugyldighedsbetingelser. I ansættelsesforhold giver det anledning til en række problemstillinger, som f.eks. opbevaring og anvendelse af personlighedstests etc.

I forhold til finansielle virksomheder er det helt afgørende, at det fastslås, at skævhed/afhængighed ikke er til stede i forholdet mellem en kunde/potentiel kunde og den finansielle virksomhed. Den finansielle virksomhed skal fortsat have mulighed for at indhente et gyldigt samtykke til behandling og videregivelse af oplysninger.

Artikel 15 - retten til indsigt

Det fremgår af artikel 15, stk. 1, at "Den registrerede har til enhver tid ret til efter anmodning at få bekræftet fra den registeransvarlige, om personoplysninger vedrørende vedkommende behandles." Vi finder, at denne artikel bør suppleres med en bestemmelse i stil med den nuværende persondatalovs § 33, hvorefter den registrerede først har krav på indsigt "6 måneder efter sidste meddelelse, medmindre der godtgøres en særlig interesse heri".

Artikel 17 og 18 – retten til at blive glemt og dataportabilitet

Forslaget til forordning indfører en række helt nye og mere vidtgående rettigheder, f.eks. artiklerne 17 og 18, der omhandler retten til at blive glemt og adgangen til dataportabilitet. Vi finder, at udkastet er uklart formuleret på disse områder, og at det ikke er oplagt, hvordan man skal forholde sig til omfanget af disse rettigheder. Der er brug for en præcisering af disse bestemmelser, f.eks. i forhold til undtagelsesbestemmelserne til retten til at blive glemt.

Bestemmelserne kan i sin nuværende form komme til at betyde, at realkreditinstitutterne skal opdele modtagne oplysninger i, hvad der skal slettes efter færdigbehandling af en given efterspørgsel, eller hvis kunden tilbagekalder et samtykke. Derudover vil der også være behov for, at kunne adskille de oplysninger, som institutterne skal slette, og de oplysninger, som institutterne er forpligtede til at opbevare i henhold til anden lovgivning, f.eks. registreringer i forhold til forpligtelser i hvidvasklovgivningen.

Artikel 31 - anmeldelse af brud på datasikkerheden

Det fremgår af artikel 31, stk. 1, at "Ved brud på persondatasikkerheden anmelder den registeransvarlige uden unødig forsinkelse og om muligt senest 24 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til tilsynsmyndigheden. Anmeldelsen til tilsynsmyndigheden ledsages af en begrundelse, hvis den ikke er indgivet inden for 24 timer."

I artikel 4, nr. 9, defineres "brud på persondatasikkerheden" som "brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet udbredelse af eller adgang til personoplysninger, der er videregivet, lagret eller på anden måde behandlet."

Vi mener, at det bør overvejes at tilføje en bagatelgrænse til denne definition.

Udover 24-timers fristen er der også krav i artikel 31, stk. 3, litra a-e, om, at meddelelsen skal indeholde en række oplysninger, herunder en beskrivelse af konsekvenser og afhjælpningsforanstaltninger.

Det forekommer som en noget urealistisk og uhensigtsmæssig frist, da de fornødne oplysninger næppe foreligger inden for 24 timer. Den dataansvarlige bør mere hensigtsmæssigt anvende ressourcer på at analysere og begrænse skaden, frem for at bruge kræfter på anmeldelse af bruddet.

Artikel 33 – konsekvensanalyse vedrørende databeskyttelse

Det fremgår af artikel 33, stk. 1, at "Hvis behandlingen af personoplysninger kan indebære specifikke risici for registreredes rettigheder og frihedsrettigheder i medfør af dens karakter, omfang eller formål, gennemfører den registeransvarlige eller den registerfører, der handler på den registeransvarliges vegne, en konsekvensanalyse af den planlagte behandling, for så vidt angår beskyttelse af personoplysninger."

Dette vil uundgåeligt medføre øgede administrative omkostninger, men omfanget heraf er uklart på grund af de meget brede og upræcise formuleringer.

Artikel 35 - databeskyttelsesansvarlige

Artikel 35 indebærer, at der fremover skal udpeges såkaldt "databeskyttelsesansvarlige" i blandt andet større virksomheder (over 250 beskæftigede).

Denne forpligtelse eksisterer ikke i dag, og ud fra artiklerne 36 og 37 virker det umiddelbart som ganske omfattende administrative opgaver, der skal varetages af den databeskyttelsesansvarlige. Der er brug for en nærmere analyse af de administrative omkostninger ved dette forslag.

Derudover er det betænkeligt, at Kommissionen mener, at der skal være tale om en særlig databeskyttelsesansvarlig. Det er uhensigtsmæssigt, at der på de enkelte områder skal oprettes en ny funktion. Det er en uhensigtsmæssig tendens, hvis Kommissionen vil kræve, at der skal udpeges en særlig ansvarlig for samtlige ansvarsområder.

Artikel 39 - certificering

Det fremgår af artikel 39, at der stilles krav om, at virksomhederne i højere grad bruger certificeringer. Det egentlige omfang af denne bestemmelse er dog stadig uklart, da Kommissionen i bestemmelsen tillægges beføjelser til at vedtage de nærmere forhold omkring anvendelsen af denne bestemmelse samt mulighed for at fastsætte de nødvendige tekniske standarder.

Derudover er det uklart, hvorfor der skulle være behov for en certificeringsordning. Kontrol af virksomhedernes overholdelse af lovgivningen bør som hidtil være en tilsynsopgave.

Artikel 79 - administrative sanktioner

Artikel 79 indeholder reglerne om administrative sanktioner. Det fremgår af artikel 79, stk. 2, at "Den administrative sanktion skal være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning."

Det foreslåede niveau for disse bøder (op til 1.000.000 EUR eller 2 pct. af omsætningen) forekommer imidlertid meget højt og ude af proportioner. Det kan blandt andet nævnes, at der i henhold til artikel 79, stk. 4, kan udstedes en bøde på op til 250.000 EUR eller 0,5 pct. af den globale omsætning, hvis den dataansvarlige ikke i tilstrækkelig grad opfylder betingelserne vedrørende indsigtsret.

Vi har noteret os, at Justitsministeriet i grundnotatets pkt. 4 angiver, at "for Danmarks vedkommende vil anvendelsen af sanktioner som nævnt i forslagets artikel 79 i givet fald skulle ske i form af udenretlige bødeforlæg. Datatilsynet har ikke en sådan adgang efter gældende ret, og det vil således kræve en lovændring med henblik på at etablere denne adgang i overensstemmelse med forslaget."

Dette underbygger blot, at det ikke er dansk retstradition, at en administrativ myndighed har mulighed for at udstede bøder i denne størrelsesorden. Vi er derfor enige i Justitsministeriets bemærkning i grundnotatets pkt. 8 om, at dette element af forslaget må overvejes "med henblik på at sikre, at de foreslåede administrative sanktionsniveauer er i overensstemmelse med proportionalitetsprincippet."

Artikel 86 - delegerede retsakter

Det fremgår af udkastets art. 86, stk. 2, at der er delegeret beføjelser til Kommissionen på hele 26 områder. Lignende lovgivningsmæssige løsninger er set på andre nylige retsakter, f.eks. i CRD IV-forslagene, men er ikke desto mindre problematiske.

En så massiv delegation til Kommissionen af den videre regulering (detailregler) efterlader et ufuldstændigt indtryk af forordningen. Det skaber endvidere en stor usikkerhed omkring muligheden for, at medlemsstaterne og dermed de nationale interessenter vil blive inddraget i tilstrækkelig grad.

Vi kan derfor støtte, at Justitsministeriet i grundnotatets pkt. 8 nævner omfanget af de delegerede retsakter som et af de elementer, hvis rækkevidde og nærmere indhold må søges afklaret under de kommende forhandlinger.

Vi står naturligvis til rådighed, såfremt Justitsministeriet har uddybende spørgsmål til vores høringssvar.

Med venlig hilsen

Jeppe Torp Vestentoft
Realkreditrådet

Heidi Holmberg
Realkreditforeningen

Landsorganisationen i Danmark
Danish Confederation of Trade Unions

Islands Brygge 32D
Postboks 340
2300 København S

Telefon 3524 6000
Fax 3524 6300
E-mail lo@lo.dk

Jmt. modt.

27 JUNI 2012

Justitsministeriet
Civil- og Politiafdelingen
Slotsholmsgade 10
1216 København K

Sagsnr. 12-1394
Vores ref. JRB
Deres ref. 2012-3756-0005

Den 26. juni 2012

Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

LO er ved skrivelse af 11. maj 2012 anmodet om eventuelle bemærkninger til forslag til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

LO kan fuldt ud tilslutte den generelle beskrivelse af kravene til behandling af personoplysninger, der fremgår af forordningsforslagets betragtning nr. 30.

Heri anføres: "Enhver behandling af personoplysninger bør udføres lovligt, loyalt og gennemsigtigt i forhold til de berørte personer. De specifikke formål med behandlingen af oplysningerne bør navnlig være udtrykkelige og legitime og fremgå, når oplysningerne indsamles. Oplysningerne bør være passende, relevante og begrænset til det minimum, der er nødvendigt til formålene med behandlingen af oplysningerne; det kræver navnlig, at det sikres, at de indsamlede oplysninger ikke er for omfattende, og at perioden for opbevaring af oplysningerne begrænses til et strengt minimum. Personoplysninger bør kun behandles, hvis formålet med behandlingen ikke kan opfyldes på anden måde. Der bør træffes enhver rimelig foranstaltning for at sikre, at personoplysninger, som ikke er nøjagtige, berigtiges eller slettes. For at sikre, at oplysningerne ikke opbevares i længere tid end nødvendigt, bør den registeransvarlige indføre tidsfrister for sletning eller periodisk gennemgang."

Forslaget indeholder en række forbedringer jfr. neden for under pkt. 5. Imidlertid overskygger forringelserne i betydelig grad disse forbedringer:

1. Forordningen skal erstatte det gældende databeskyttelsesdirektiv. Ændringen af retligt instrument giver anledning til betydelig bekymring i relation til mulighederne for at opretholde de hidtidige særregler og ikke mindst de regler, der er særegne for det danske arbejdsmarked med en udpræget aftaleregulering. Denne bekymring er udtalt af andre, således bl.a. af direktøren for Datatilsynet, der den 25.1 2012 har udtalt:

"Vi er umiddelbart noget skeptiske over for valget af en forordning i stedet for et direktiv. Forordningen kan være et godt valg på områder med grænseoverskridende ydelser, men måske ikke som et generelt instrument på alle områder. Der er meget store forskelle landene imellem – historisk og kulturelt betinget" … "Med forordningen falder den dan-

ske persondatalov helt bort, dvs. også de ganske fornuftige særregler, som vi har haft i Danmark i mange år, og som ikke har givet anledning til problemer. Samtidig giver forslaget mere magt til EU-kommissionen og til et "overdatatilsyn" på EU-niveau"

Ændringen er endvidere behandlet indgående af professor, dr. jur. Peter Blume i Juristen 2012, side 57 ff (Direktiv eller forordning i persondataretten). Blume anfører side 58 bl.a. følgende:

"Når en forordning udstedes, kan der på nationalt niveau foreligge to situationer, idet der kan være glidende overgange mellem dem. Det ene yderpunkt er, at der er tale om et emne, som ikke hidtil er blevet retligt reguleret. Dette er retsteknisk enkelt, idet forordningen uden videre udfylder det tomme rum. I dag er der ikke mange af disse rum. Det andet yderpunkt er, at der i forvejen findes en national regulering, der må forsvinde som følge af forordningen. Dette er det typiske og er også tilfældes for persondataretten. Her må det således nøje overvejes, hvilke regler der må falde og hvilke der kan stå" ... "Det kan yderligere tilføjes, at problemstillingen også er aktuel på områder, hvor den retlige regulering eller i hvert fald dele af den ikke er fastsat ved lov. Hovedeksemplet er **det arbejdsretlige område**, hvor det derfor må vurderes, om den praksis, der er udviklet på basis af en kombination af ledelsesretten og den omgivende lovgivning, kan opretholdes, eller om den er opslugt af forordningen. Dette vil heller ikke blive en nem øvelse, selvom der ifølge forslagets artikel 82 nationalt kan fastsættes regler om behandling af oplysninger om ansatte. (Udhævet her)."

EU-forslaget og dets konsekvenser for arbejdsmarkedet er endvidere blevet behandlet af Peter Blume og professor, dr. jur. Jens Kristiansen på et foredrag den 12.4 2012. Her blev de samme betænkeligheder som oven for nævnt fremført. LO vedlægger slides fra mødet, da der ikke foreligger manuskript.

2. Europa-Kommissionen har tidligere overvejet et specifikt direktiv for arbejdsmarkedet. Denne opfattelse er nu forladt med det foreliggende forslag. Af betragtning nr. 124 fremgår det, at "De generelle principper vedrørende beskyttelse af fysisk personer i forbindelse med behandling af personoplysninger også bør gælde i ansættelsesforhold".

Som følge heraf er der som hjemmel for forslaget angivet art. 16 og 114, stk. 1, i TEUF. Art. 153-155 foreskriver imidlertid en særlig fremgangsmåde med udpræget indflydelse for arbejdsmarkedets parter, når det drejer sig om regulering af arbejdsmarkedet. Det er særdeles uheldigt, at denne indflydelse hindres ved at placere en regulering af et arbejdsmarkedsområde i en generel forordning om persondata. Man burde derfor undtage ansættelsesforhold og indgåelse og overholdelse af kollektive overenskomster fra forordningens anvendelsesområde. Dette kan ske ved at medtage området i forslagets art 2, stk. 2, om den behandling af personoplysninger, forordningen ikke gælder for.

3. LO er opmærksom på forslagets art. 82. Herefter kan "medlemsstaterne vedtage specifikke bestemmelser, der regulerer behandlingen af arbejdstagernes personoplysninger i ansættelsesforhold."

Imidlertid er der i hvert fald 3 problemer med denne bestemmelse. For det første er medlemsstaterne adgang begrænset til: "under overholdelse af denne forordning". Spørgsmålet er, hvad der nærmere ligger heri og hvilke begrænsninger, der helt præcist følger heraf i forhold til den hidtidige danske regulering.

For det andet nævner bestemmelsen ikke de kollektive aftaler, der i betydeligt omfang regulerer arbejdsgiverens behandling af persondata i Danmark. Der er således aftaler på Hovedorganisationsniveau (fx aftalen mellem DA og LO om kontrolforanstaltninger), regulering af fx videoovervågning i de kollektive fagoverenskomster og vedtagelser i Samarbejdsudvalg om fx e-mailpolitik og brug af internet samt kontrol heraf. Det er helt afgørende for den danske model, at art. 82 kan rumme alle disse aftaler.

For det tredje har kommissionen adgang til efter art. 82, stk. 3, at udstede nærmere retningslinjer for vedtagelsen af nationale regler. Spørgsmålet er hvilke begrænsninger medlemsstaterne kan pålægges herved.

4. Som nævnt oven for er der tvivl om hvilke af de danske særregler, der vil kunne opretholdes i tilfælde af, at der vedtages en forordning i stedet for som hidtil et direktiv.

a) Blume nævner a. st. side 58 f reglen i persondatalovens § 1, stk. 2. Denne regel om manuel (ikke-elektronisk, systematisk behandling) har på det arbejdsretlige område betydning for personalemapper i papirform. Det er særdeles vigtigt, at også en sådan indsamling af oplysninger er undergivet beskyttelsesreglerne. Bemærkningerne i betragtning nr. 13 kunne umiddelbart tyde på, at dette var tilfældet. Det har imidlertid ikke fundet klart udtryk i forslaget til art. 4, nr. 3.

b) Oluf Jørgensen fremhæver i en pressemeddelelse af 30.3 2012 hensynet til informations- og ytringsfriheden. Man må herved fremhæve persondatalovens § 2, stk. 2, der netop sikrer disse friheder.

c) I en arbejdsretlig sammenhæng er reglen i § 7, stk. 3, i persondataloven om oplysninger om fagforeningsmæssige tilhørsforhold vigtig. Reglen ses imidlertid gentaget i forslagets art. 9, stk. 2, litra b.

d) Persondatalovens § 8, stk. 1, indeholder et forbud mod at behandle "oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold". Disse oplysninger er ikke indeholdt i forslaget til art 9, stk. 1, hvad der indebærer en væsentlig reduktion af beskyttelsesniveauet.

e) Persondatalovens § 11 regulerer behandlingen af personnumre både i relation til offentlige myndigheder og private, herunder arbejdsgiveres behandling. Forordningsforslaget nævner ikke personnumre, hvilket ifølge Blume a. st. side 60 "har den konsekvens, at denne oplysning reguleres som en almindelig personoplysning, hvor der er flere muligheder for at behandle den uden samtykke". Dette er ikke acceptabelt.

f) Afsnit V i persondataloven indeholder regler om anmeldelse forinden behandling af oplysninger. Disse regler udgår af forordningen. Betragtning nr. 70 i forslaget behandler denne ændring. Argumentationen for udeladelsen forekommer ikke overbevisende.

g) Særligt bemærkes reglen i afsnit V i persondatalovens § 50 om advarselsregistre. Denne regel regulerer i § 50, stk. 1, nr. 2, behandlingen af oplysninger, der sker med henblik på at advare andre mod ansættelsesforhold. Det er særdeles beklageligt, hvis der i fremtiden kan oprettes sådanne advarselsregistre uden forudgående tilladelse fra Datatilsynet.

5. a. LO har med tilfredshed noteret sig de skærpede regler om samtykke i forslagets art 7 og de tilhørende bemærkninger i betragtning nr. 25 og nr. 32-34.

b. LO har tilsvarende noteret sig kravene til den registeransvarlige i forslagets art 11-14.

c. LO har tilsvarende noteret sig forlagene til forbedrede regler om registreredes rettigheder; især i art 15, 17, 18 og 19.

Med venlig hilsen

Marie-Louise Knuppert

Landsorganisationen i Danmark
Danish Confederation of Trade Unions

Islands Brygge 32D
Postboks 340
2300 København S

Telefon 3524 6000
Fax 3524 6300
E-mail lo@lo.dk

Jmt. modt.
-9 JULI 2012

Justitsministeriet
Civil- og Politiafdelingen
Slotsholmsgade 10
1216 København K

Sagsnr. 12-1394
Vores ref. MLK/JRB/sea
Deres ref.

Den 6. juli 2012

Høring over Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

LO har den 26. juni 2012 sendt et høringssvar med bemærkninger til forslaget. LO ønsker at supplere dette høringssvar, idet vi efterfølgende fra medlemsforbundene har modtaget yderligere bemærkninger.

1. En række artikler er afgrænset til at finde anvendelse på virksomheder og organisationer med 250 beskæftigede eller derover. Det gælder fx artikel 28 om dokumentationskrav og artikel 35 om udpegning af en databeskyttelsesansvarlig.

LO finder, at en tærskel på 250 beskæftigede er for høj. Konsekvensen vil være, at de fleste danske virksomheder som udgangspunkt ikke omfattes af de pågældende artikler i forslaget.

2. Der synes ikke i forslaget at være artikler, der sikrer de krænkedes rettigheder. LO finder, at forslaget burde indeholde en hjemmel til at sikre, at krænkede kan tilkendes en godtgørelse.

3. Artikel 39 omhandler certificerings- og mærkningsordninger. LO noterer med tilfredshed, at der tilskyndes til at indføre sådanne ordninger.

Det er ikke klart, om artikel 39 giver hjemmel til at stille krav om certificering af firmaer, der leverer udstyr til elektronisk overvågning, herunder tv-overvågning.

LO finder, at det bør afklares, og hvis hjemmelen ikke rækker hertil, ønsker LO den udvidet.

4. I forordningens kap. VIII (artikel 73, stk. 2 og 3) omtales en ret for bl.a. organisationer til at indgive en klage på vegne af den registrerede til en national tilsynsmyndighed. Det er et krav, at de pågældende organisationer er "etableret i overensstemmelse med en medlemsstats lovgivning" (stk.2).

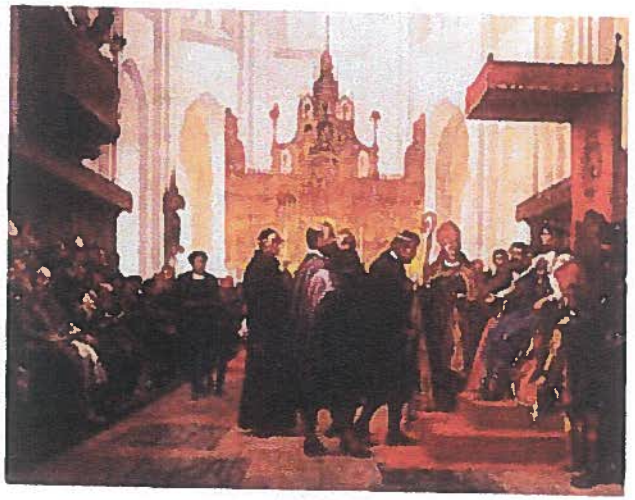
Det bør overvejes at ændre teksten, således at faglige organisationer ikke udelukkes fra at indgive klager på vegne af medlemmerne.

Med venlig hilsen

Marie-Louise Knuppert

Det nye EU-forslag til forordning om persondatabeskyttelse og dets konsekvenser for arbejdsmarkedet

Professor, dr. jur. Peter Blume og
professor, dr. jur. Jens Kristiansen



Ny persondataret

Med særligt sigte på arbejdsmarkedsrelaterede forhold

Ved professor, dr. jur. Peter Blume

Mødet mellem to retstraditioner

- det kollektive og det individuelle

Gældende regulering:

- direktiv 95/46 EF

Grundlæggende rettighed:

- Charter artikel 8
- TEUF artikel 16

Regler, der forsvinder:

Persondataloven

- § 1, stk.2: systematisk behandling
- § 50: advarselsregistre
- § 8: strafbare forhold
- § 11: personnumre
- Anmeldelsesordningen

Bliver bedre regler stående?

- 6 ugers varslings regel

Nye regler:

- samtykke: ikke væsentlig skævhed
- organisationer og de registrerede
- ny funktion: databekyttelesansvarlig

Artikel 82(1):

"Under overholdelse af denne forordning kan medlemsstaterne vedtage specifikke bestemmelser, der regulerer behandlingen af arbejdstageres personoplysninger i ansættelsesforhold, blandt andet i forbindelse med ansættelse, ansættelseskontrakter, herunder godtgørelse for forpligtelser fastsat ved lov eller kollektive overenskomster, arbejdets ledelse, planlægning og tilrettelæggelse, arbejdsmiljø, og i forbindelse med individuel eller kollektiv udøvelse og brug af rettigheder og fordele i forbindelse med ansættelse og i forbindelse med ophør af ansættelsesforhold"

- Artikel 82(3): Kommissionen kan uddybe stk. 1 i delegeret retsakt.

- Generel EU interesse
- Vær beredt!

Det nye persondataforslag i arbejdsretligt perspektiv

Ved professor, dr. jur. Jens Kristiansen

I Danmark er arbejdsgiveres behandling af persondata

- fortsat ikke underlagt specifik arbejdsretlig lovgivning (bortset fra helbredsoplysningsloven)

- men i det væsentlige stadig baseret på kollektive aftaler, ledelsesretten og samarbejdsudvalgssystemet

Markant udvikling i de persondataretlige regler

- Registerlovene fra 1970'erne

- Persondataloven fra 2000
  - baseret på direktiv 46/1995
  - men tilpasset danske forhold

- Nyt forslag til forordning 2012
  - ensartet grundlag for behandling af persondata i EU
  - vægt på grundlæggende rettigheder og effektiv retshåndhævelse

EU og arbejdsmarkedet

- Unionen "støtter og supplerer medlemsstaternes indsats" på det arbejdsmarkedsmæssige område, jf. TEUF artikel 153

- Særlig model for EU-regler på arbejdsmarkedet
  - kun hjemmel til direktiver med mindsteforskrifter
  - forhandlings- og aftaleret for organisationerne
  - implementering via lov og/eller overenskomster

- Persondatadirektivet vedtaget med andet hjemmelsgrundlag
  - og Kommissionens initiativ til et specifikt direktiv for arbejdsmarkedet blev aldrig formelt fremsat

Forslaget til persondataforordning

- Forslaget baserer sig på (ny) specifik hjemmel i TEUF artikel 16 om persondatabeskyttelse
- Bestemmelsen giver adgang til langt mere vidtgående harmonisering end TEUF artikel 153-55
  - Kommissionen kan vælge forordning frem for direktiv
  - ingen forhandlings- og aftaleret for organisationerne
  - en forordning skal ikke implementeres nationalt

Særligt hensyn til arbejdsmarkedet i artikel 82

- Anerkender arbejdsmarkedet som et særligt område, men er tavs om "retten til kollektive forhandlinger"
- Giver medlemsstaterne hjemmel til (at vedtage) regler om persondata i ansættelsesforhold
- Men de nationale regler skal gennemføres inden for rammerne af forordningen
- Og Kommissionen kan udstede nærmere retningslinjer for vedtagelsen af nationale regler

Forslagets model er vidtgående – også for arbejdsmarkedet

Medlemsstaterne kan vælge mellem

- at følge de fuldt ud harmoniserede regler for håndtering af persondata i EU

eller

- at tilpasse reglerne via "specifikke bestemmelser" under "overholdelse af denne forordning"

Er der alternative muligheder?

- Direktiv i stedet for forordning
- Udvidet adgang til nationale (overenskomstmæssige) tilpasninger for persondata i ansættelsesforhold (artikel 82)
- Undtage ansættelsesforhold fra forordningens anvendelsesområde (artikel 2)

Høringssvar

27.06.2012

Kontakt: Helle Bronth Bentz - brb@ftf.dk - Tlf: 3336 8800

Vidtgående EU-forslag om persondatabeskyttelse.

Europa-Kommissionen har fremsat forslag til forordning om persondatabeskyttelse. I forhold til den danske persondatalov indeholder forslaget en række forbedringer, men desværre også væsentlige forringelser og ikke mindst uklarheder om forslagets rækkevidde.

FTF har modtaget Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (genere forordning om databeskyttelse, KOM (2012) 11) i høring og har følgende bemærkninger:

Indledningsvis bemærkes, at der er tale om et forordningsforslag, som efter sit indhold bl.a. har til formål at ophæve og erstatte det gældende databeskyttelsesdirektiv (direktiv 95/46/EF). Med forslaget om en forordning ønsker Kommissionen at skabe "en stærk og retlig ramme" på området på tværs af EU's politikker.

Databeskyttelse er en grundlæggende rettighed, som således skal beskyttes.

Det er derfor positivt, at EU-Kommissionen har fokus på at forbedre persondatabeskyttelsen med henblik på at sikre et højt og effektivt samt mere ensartet databeskyttelsesniveau for fysiske personer, som tillige skal fremme retssikkerheden.

Men med udstedelsen af en forordning frem for som hidtil et direktiv, ophæves og bortfalder den danske persondatalov nødvendigvis, og dermed også de særregler, som har været gældende i Danmark i mange år, ikke mindst på det arbejdsretlige område, der som bekendt er præget af aftaleregulering frem for lovregulering.

Som hjemmelsgrundlag henviser forslaget blandt andet til art. 16 i TEUF om persondatabeskyttelse. Denne bestemmelse giver imidlertid adgang til en langt mere vidtgående harmonisering end TEUF art. 153-155, hvorefter arbejdsmarkedets parter har mulighed for at opnå indflydelse på arbejdsmarkedspolitiske forhold. FTF finder det derfor særdeles beklageligt, at Kommissionen vælger at foretage reguleringen af arbejdsmarkedspolitiske forhold i en forordning frem for et direktiv, hvorved parterne afskæres fra at udøve denne indflydelse.

FTF er naturligvis opmærksom på forslagets artikel 82, hvorefter medlemsstaterne – fortsat - kan vedtage specifikke bestemmelser, der regulerer behandlingen af arbejdstageres personoplysninger i ansættelsesforhold.

Men for det første fremgår det, at sådanne specifikke regler og aftaler skal overholde forordningen. Det er ganske uklart, hvad der ligger heri, og hvilke begrænsninger dette krav om overholdelse indeholder i forhold til den hidtidige regulering i Danmark.

For det andet hjemler forslagets artikel 82, stk. 3, adgang for Kommissionen til at udstede nærmere retningslinier for vedtagelsen af nationale regler. Det fremgår imidlertid ikke, hvilke begrænsninger, der kan pålægges herved.

Det er på den baggrund FTF's opfattelse, at forordningsforslaget skaber betydelige uklarheder i forhold til reguleringen – såvel den legale som aftaleretlige – af det danske arbejdsmarked.

FTF opfordrer derfor til at være opmærksom på de alternative muligheder, der findes til forslaget om at udstede en forordning:

1. Udstedelse af nyt direktiv specifikt for arbejdsmarkedet, hvilket Europa-Kommissionen tidligere har overvejet.

2. Indførelse af en udvidet adgang til nationale - såvel lovgivningsmæssige som aftalebaserede - tilpasninger for personoplysninger i ansættelsesforhold, jfr. forordningsforslagets art. 82.

3. Undtagelse af ansættelsesforhold og den aftalebaserede regulering af arbejdsmarkedsforhold fra forordningsforslagets anvendelsesområde, jfr. forslagets art. 2, stk. 2.

Det er FTF's opfattelse, at disse alternativer kan indeholdes i opbygningen af den "moderne, stærke, sammenhængende og omfattende databeskyttelsesramme for den Europæiske Union", som EU lægger op til.

Forordningsforslaget indeholder en række nyskabelser set i forhold til det gældende direktiv, ligesom forslaget gentager en række af de gældende bestemmelser.

Det er positivt, at forslaget blandt andet skærper kravene til samtykke som behandlingsgrundlag, jfr. art. 7. I følge forslaget vil et samtykke ikke kunne tilvejebringe det fornødne retsgrundlag for en behandling, hvis der er en "klar skævhed mellem den registrerede og den registeransvarlige". Af præambelbetragtning (34) fremgår, at en sådan skævhed navnlig foreligger, når den registrerede befinder sig i et afhængighedsforhold til den registeransvarlige, herunder når personoplysninger behandles af en arbejdsgiver som led i et ansættelsesforhold.

Desuden ses den nuværende regel i persondatalovens § 7, stk. 3, om behandlingen af oplysninger om fagforeningsmæssige tilhørsforhold gentaget i forslagets art. 9, stk. 2. Sådanne oplysninger vil fortsat henhøre i kategorien følsomme oplysninger, hvilket FTF fuldt ud kan tilslutte sig.

Endvidere kan FTF tilslutte sig forslagets nyskabelser i relation til den registreredes rettigheder, jfr. forslagets kapitel III.

Det samme gælder den nye funktion som databeskyttelsesansvarlig, jfr. kapitel IV. Eftersom den databeskyttelsesansvarlige også har kontrolforanstaltninger over den registeransvarlige, bør det derfor overvejes at indføre en beskyttelse af den databeskyttelsesansvarlige i de tilfælde, hvor den databeskyttelsesansvarlige er ansat af den registeransvarlige - på lige fod med den særlige beskyttelse, der gælder for f.eks. arbejdsmiljø- og tillidsrepræsentanter.

Men forslaget indeholder imidlertid også en række forringelser, og f.eks. reduceres beskyttelsesniveauet, når det drejer sig om at behandle oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold. Disse oplysninger, som i dag fremgår af persondatalovens § 8, stk. 1, ses ikke indeholdt i forslaget, og det finder FTF uacceptabelt. Sådanne oplysninger skal derfor omfattes af art. 9.

Det samme gælder behandlingen af personnumre, som er reguleret i persondatalovens § 11. § 11 regulerer også arbejdsgiveres behandling af personnumre, men forordningsforslaget nævner ikke personnumre. Det har alt andet lige den konsekvens, at oplysninger om personnumre vil blive reguleret som en ikke-følsom personoplysning, hvilket giver flere muligheder for at behandle uden samtykke. FTF foreslår derfor, at personnumre konkret omfattes af art. 9.

Endvidere udgår reglerne persondatalovens afsnit V om anmeldelse forinden behandling af oplysninger. Forslagets begrundelse herfor forekommer hverken saglig eller relevant, hvilket er så meget desto mere beklagelig henset til, at afsnittet også indeholder reglen i § 50 om advarselsregistre. § 50 har stor relevans for arbejdsmarkedet, og FTF finder det særdeles utilfredsstillende, hvis der ikke længere gælder krav om forudgående tilladelse fra Datatilsynet, forinden sådanne advarselsregistre oprettes.

Ud over de ovenfor anførte betragtninger kan FTF desuden i det hele henholde sig til bemærkningerne i såvel Dansk Sygeplejeråd's høringssvar som LO's høringssvar af den 26. juni 2012.

Med venlig hilsen

Bente Sorgenfrey
Formand

Fra: Christoffer Greenfort [cgr@travelassoc.dk]
Sendt: 28. juni 2012 14:39
Til: 'intsek@evm.dk'; Justitsministeriet
Cc: Jakob Hahn
Emne: SV: Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttel

Mange tak for det tilsendte materiale, og muligheden for at komme med bemærkninger.

DRF har på nuværende tidspunkt ingen specifikke kommentarer eller bemærkninger, men venter spændt på de kommende analyser, og det ekstra materiale, der måtte blive udarbejdet til forslaget.

Ser frem til at modtage yderligere i fremtiden.

Med venlig hilsen / Kind regards

Christoffer Greenfort
Juridisk konsulent / Legal advisor
Cand.Jur / LLM

Danmarks Rejsebureau Forening
(Association of Danish Travel Agents and Tour Operators)

Vodroffsvej 32
1900 Frederiksberg C
E-mail: cgr@travelassoc.dk
Phone.: (+45) 35 30 12 56
Telefax.: (+45) 35 35 88 59
CVR. Nr.: 20 77 03 17
www.travelassoc.dk

Fra: Jakob Hahn
Sendt: 21. maj 2012 12:44
Til: Christoffer Greenfort
Emne: VS: Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttel

Vil du kigge denne igennem og lægge deadline i kalenderen

Mvh
Jakob

Fra: Danmarks Rejsebureau Forening

Justitsministeriet
Slotsholmsgade 10
1216 København K
jm@jm.dk
Vedr. j.nr. 2012-3756-0005

Dato 28. juni 2012
Jnr 01.22.00 K04
Sagsid 000241966

Ref ABN
abn@kl.dk

Weidekampsgade 10
Postboks 3370
2300 København S

Tlf 3370 3370
Fax 3370 3062

www.kl.dk

KL's høringssvar vedr. Kommissionens forslag til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

Ved brev af 11. maj 2012 har Justitsministeriet anmodet KL om at modtage eventuelle bemærkninger i anledning af Kommissionens forslag til generel forordning om databeskyttelse.

KL skal i den anledning udtale følgende:

- *Direktiv frem for forordning*

Det er KL's principielle opfattelse, at reglerne om databeskyttelse bør være indeholdt i et direktiv og ikke i en forordning. Det giver Danmark bedre muligheder for selv at vælge, hvilke midler der skal anvendes for at implementere reglerne, og det giver Danmark mulighed for at opretholde det danske kollektive arbejdsretlige aftalesystem, som vi kender det i dag, jf. nærmere herom nedenfor.

Der er desuden i forordningen valgt en model, hvor Kommissionen i meget vidt omfang får adgang til at udstede retsakter, hvor Kommissionen fastlægger kriterier og betingelser i forhold til de enkelte bestemmelser i forordningen, jf. artikel 86. De nærmere rammer for indholdet af de delegerede retsakter fremgår ikke af forordningen. Det betyder, at Kommissionens mulighed for at vedtage delegerede retsakter giver en høj grad af usikkerhed om, hvad der er og vil blive gældende ret. KL frygter, at Kommissionen vil vedtage et betydeligt antal regler, som ikke i nødvendigt omfang vil tage højde for særlige forhold i den offentlige sektor og på ansættelsesområdet mv.

Hertil kommer, at Kommissionens beføjelser efter den generelle forordning til bl.a. at udforme blanketter, fastsætte formater, fastsætte tekniske standarder mv. vil medføre unødige omkostninger for kommunerne som regi-

steransvarlige, der efterfølgende vil skulle betale for at få deres it-systemer, herunder selvbetjeningsløsninger, tilpasset sådanne krav.

En væsentlig begrundelse for Kommissionens forslag til en forordning er ønsket om at skabe et ensartet og styrket databeskyttelsesniveau i medlemslandene med henblik på, at forbrugerne får mere tillid i onlinemiljøet, så borgerne ikke er tilbageholdende med at købe varer på internettet og benytte online tjenester, ligesom virksomhederne har brug for klare, ensartede regler i medlemslandene.

KL anerkender, at der i forhold til virksomheder kan være behov for ensartede regler i EU, navnlig for virksomheder, der driver virksomhed i flere medlemsstater.

Det er imidlertid KL's opfattelse, at forordningen rammer uhensigtsmæssigt i forhold til offentlige myndigheder og i forhold til det ansættelsesretlige område, hvor hovedparten af de persondatabehandlinger, der foretages, er rent nationale. KL finder på den baggrund ikke, at en retsakt i form af en forordning kombineret med Kommissionens mulighed for at udstede yderligere regler tilgodeser nærhedsprincippet.

KL foreslår derfor, at private virksomheders brug af borgernes data reguleres i en forordning og offentlige myndigheders behandling af persondata og det ansættelsesretlige område undtages fra den generelle forordnings anvendelsesområde efter forordningens artikel 2, stk. 2, således at offentlige myndigheders behandling af persondata og det ansættelsesretlige område fortsat reguleres i et direktiv. Da der i det gældende databeskyttelsesdirektiv (95/46/EF af 24. oktober 1995) er en række uklarheder, vil der være behov for, at dette direktiv revideres.

Såfremt Kommissionens ønske om en forordning fastholdes på det ansættelsesretlige område og for offentlige myndigheders behandling af persondata, ønsker KL følgende ændringer af forordningen:

- *Administrative byrder og meromkostninger*

Forordningen vil medføre nye administrative byrder og meromkostninger for kommunerne, der efter KL's opfattelse ikke står mål med de gevinster, borgerne vil opleve. Samtidig vurderer KL, at forordningen vil besværliggøre og fordyre realiseringen af potentialerne i den fællesoffentlige digitaliseringsstrategi for 2011-2015, "Den digitale vej til fremtidens velfærd", særligt strategiens fokusområde om den digitale kommunikation med borgerne.

KL ønsker, at de administrative byrder i forordningen helt eller delvist fjernes i forhold til kommunerne, herunder kommunerne som arbejdsgiver.

Det drejer sig fx om følgende:

- Pligt til at indhente borgerens samtykke ved brug af selvbetjeningsløsninger på nettet (artikel 4, nr. 8 og præambel nr. 25)
- Pligt til at sikre, at borgere kan overføre data til et andet databehandlingssystem (artikel 18)
- Nye dokumentationskrav til databehandlingen (artikel 28)
- Udvidede rettigheder for borgerne med øgede, administrative opgaver for kommunerne til følge, fx ret til kopi af behandlinger m.m.
- Pligt til at anmelde brud på datasikkerheden til tilsynsmyndigheden (artikel 32)
- Pligt til at udarbejde konsekvensanalyser af risikofyldte databehandlinger (artikel 33)
- Pligt til at ansætte en databeskyttelsesansvarlig (artikel 35 – 37)
- Pligt at anvende særlige EU-blanketter

./. Der henvises til KL's bemærkninger til de enkelte artikler i vedlagte bilag til høringssvaret.

- *Det ansættelsesretlige område / den danske model*

I Danmark er arbejdsgiveres behandling af persondata ikke underlagt specifik arbejdsretlig lovgivning, men er i det væsentlige reguleret i kollektive aftaler, ledelsesretten og samarbejdsudvalgssystemet. Hensynet til denne tradition vil være vanskelig at opretholde med det foreliggende forslag til en forordning.

Forordningen giver bl.a. mulighed for, at medlemsstaterne kan "vedtage specifikke bestemmelser" for behandling af persondata i ansættelsesforhold "under overholdelse af denne forordning", jf. artikel 82. KL finder det nødvendigt, at det i forordningen præciseres, at der kan ske nationale tilpasninger for behandling af persondata i ansættelsesforhold via kollektive overenskomster, således at den danske aftalemodel kan opretholdes.

Efter KL's opfattelse bør det endvidere sikres, at arbejdsgiverens ledelsesret ikke begrænses. Navnlig skal det sikres, at kommunerne som arbejdsgiver kan behandle oplysninger som led i et ansættelsesforhold på grundlag af et samtykke fra lønmodtageren, ligesom kommunerne ikke skal begrænses i forhold til ansættelse/afskedigelse af en databeskyttelsesansvarlig.

Der henvises til uddybende bemærkninger til artikel 7, artikel 9 og artikel 82.

- *Høje bøder*

Der vil i medfør af forordningen kunne udstedes uforholdsmæssigt høje bøder til kommunerne, hvis de ikke overholder reglerne, herunder fx bøder

på 250.000 EUR (1.875.000 kr.) for manglende eller mangelfuld overholdelse af den registreredes rettigheder og bøder på 1.000.000 EUR (7.500.000 kr.), hvis der ikke udpeges en databeskyttelsesansvarlig.

De høje bødeniveauer vil efter KL's opfattelse være ganske byrdefulde for kommunerne, hvorfor KL ønsker, at bøderne ikke skal gælde for kommunerne, alternativt at bøderne skal være på et langt lavere niveau for offentlige myndigheder.

Der henvises til uddybende bemærkninger til artiklerne 78 -79.

- *Uklare regler*

Mange af forordningens regler er ikke klare nok, eksempelvis er det uklart, hvilke administrative krav det stiller til kommunerne, at personoplysninger behandles "gennemsigtigt". Et andet eksempel er, at det fremgår af forordningen, at samtykke fra den registrerede ikke kan tilvejebringe et retligt grundlag for behandling, hvis der er en klar skævhed mellem den registrerede og den registeransvarlige. Det er uklart, hvilken betydning det i praksis vil få for offentlig myndigheders mulighed for at behandle oplysninger på grundlag af samtykke.

KL ønsker, at de uklarheder, der er i forordningen, bliver afklaret. Der henvises til uddybende bemærkninger bl.a. til artikel 4, nr. 8, artikel 5 og artikel 7.

Hvis forslaget til forordning vedtages, forventer KL at rejse et DUT-krav med henblik på, at kommunerne bliver kompenseret for de øgede, administrative opgaver.

Med venlig hilsen

Erik Nielsen

BILAG

KL's bemærkninger til de enkelte artikler i Kommissionens forslag til generel forordning om databeskyttelse

Den 27. juni 2012

Jnr 01.22.00 K04
Sagsid 000241966

Ref LPJ/ABN
lpj@kl.dk
Dir 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

Tlf 3370 3370
Fax 3370 3371

www.kl.dk

Kapitel 1 – Generelle bestemmelser

Artikel 2, stk. 2, litra d og præambel nr. 15: Det bør yderligere uddybes i præambel nr. 15, hvad der skal forstås ved "rent personlige eller familiemæssige aktiviteter", herunder om fx private foreningers behandling af oplysninger er omfattet af undtagelsen.

Artikel 3: Det bør præciseres direkte i artiklen, at forordningens territoriale anvendelsesområde også omfatter registeransvarliges aktiviteter uden for Unionen, såfremt de omfatter behandling af oplysninger om registrerede bosiddende i Unionen. Præciseringen fremgår af præamblens nr. 19, men fremgår ikke tydeligt af selve forordningens ordlyd.

Artikel 4, nr. 1 og præambel nr. 23 og 24: Det er efter KL's opfattelse uklart, i hvilke situationer id-numre, lokaliseringsdata, online-id'er skal betragtes som personoplysninger, jf. formuleringen af artikel 4, nr. 1 sammenholdt med præambel nr. 23 og 24, som henholdsvis indikerer, at der kan være tale om personoplysninger (nr. 23) henholdsvis konkluderer, at id-numre, lokaliseringsdata, online id'er ikke under alle omstændigheder skal betragtes som personoplysninger (nr. 24).

Artikel 4, nr. 8 og præambel nr. 25 og 32: Et samtykke skal fremover være "udtrykkeligt". Af præambel nr. 25 fremgår, at et udtrykkeligt samtykke gives "ved hjælp af en passende metode,...." Det bør præciseres, om dette indebærer, at de registeransvarlige vil blive forpligtede til at gøre mere, herunder eventuelt indkøbe systemer til håndtering af samtykke ved brug af selvbetjeningsløsninger, end der stilles krav om i dag. Specifikke krav om afkrydsningsfelt på hjemmesider, hvor borgeren skal give specifikt samtykke

til behandlingen, vil betyde væsentlige udviklingsomkostninger for kommunerne.

Desuden fremgår det af præamblens nr. 32, at den registrerede skal have en "garanti" i forbindelse med afgivelse af sit samtykke. Her bør det ligeledes præciseres, hvilke administrative konsekvenser kravet har for kommunerne, herunder om det betyder krav om indkøb af særlige garantifunktionaliteter til indarbejdelse i kommunernes it-systemer.

Artikel 4, nr. 12 og præambel nr. 26: Det bør sikres ved formuleringen af definitionen i artikel 4, nr. 12, vedrørende helbredsoplysninger sammenholdt med præamblens nr. 26, at Datatilsynets praksis, hvorefter offentlige myndigheder via almindelig sms og e-post kan sende borgerne aftalepåmindelser og servicebeskeder, som indeholder fortrolige og/eller følsomme oplysninger, fx påmindelser om aftaler på sygehuse, misbrugscentre mv., kan opretholdes. Der henvises til Datatilsynets meddelelse af 13. september 2010 om offentlige myndigheders kommunikation med borgerne via sms.

Kapitel II Principper

Artikel 5, litra a: Denne bestemmelse indebærer et nyt krav om, at personoplysninger skal behandles "…..loyalt og på en gennemsigtig måde". Det er efter KL's opfattelse uklart, hvad der ligger heri, og hvilke krav det stiller til kommunerne som registeransvarlige.

Artikel 5, litra f: Den registeransvarlige skal "for hver behandlingsaktivitet påvise overensstemmelse med denne forordning". Det fremgår ikke klart, om dette indebærer en ny, administrativ opgave for kommunerne, ligesom det ikke fremgår klart, hvordan den registeransvarlige skal påvise overensstemmelse med forordningen.

Artikel 6, stk. 1, litra f: Offentlige myndigheder kan ifølge forslaget ikke anvende bestemmelsen i artikel 6, stk. 1, litra f, hvorefter en behandling kan være lovlig ud fra en konkret interesseafvejning. Af præamblen nr. 38 fremgår som begrundelse herfor følgende: *"Det er lovgiver, der i henhold til lovgivningen fastsætter retsgrundlaget for offentlige myndigheders behandling af oplysninger, og derfor bør dette retsgrundlag ikke gælde for den behandling, offentlige myndigheder foretager som led i udførelsen af deres opgaver."*

Det fremgår ikke klart, om denne bestemmelse vil begrænse kommunernes mulighed for at behandle oplysninger i situationer, hvor behandlingen ikke nødvendigvis sker for at overholde en retlig forpligtelse eller som led i offentlig myndighedsudøvelse. Det er navnlig tilfældet, når kommunerne behandler oplysninger som arbejdsgiver.

Som eksempel kan nævnes, at Datatilsynet har udtalt, at offentlige myndigheder og private arbejdsgivere med hjemmel i den tilsvarende bestemmelse i persondatalovens § 6, stk. 1, nr. 7, kan offentliggøre oplysninger om medarbejderes navn, stillingsbetegnelse, arbejdsområde, ansættelsesår mv. på en hjemmeside uden samtykke fra medarbejderen, se bl.a. Datatilsynets udtalelse, j.nr. 2000-216-0002. Et andet eksempel er Datatilsynets udtalelse vedrørende arbejdsgiveres mulighed for videregivelse af oplysninger om ansattes løn uden samtykke fra den ansatte, jf. Datatilsynets udtalelse j.nr. 2007-321-0047.

KL ønsker på den baggrund, at det præciseres, at bestemmelsen i artikel 6, stk. 1, litra f ikke gælder "for den behandling offentlige myndigheder foretager som led i udførelsen af opgaver, der henhører under offentlig myndighedsudøvelse".

Artikel 7 og præambel nr. 33 og 34:

Det fremstår ikke klart, hvilken betydning artikel 7, stk. 3, sammenholdt med præamblens nr. 33, hvoraf det fremgår, at samtykke skal kunne tilbagetrækkes uden, at det er til skade for den registrerede, vil få for dansk ret, herunder princippet om processuel skadevirkning, jf. bl.a. § 29 i forvaltningsloven.

Det fremgår af artikel 7, litra 4, at samtykke ikke tilvejebringer et retsgrundlag for behandling, hvis der er en klar skævhed mellem den registrerede og den registeransvarlige. Det fremgår af præambel nr. 34, at dette navnlig er tilfældet, når den registrerede befinder sig i et afhængighedsforhold til den registeransvarlige, bl.a. når arbejdsgiveren behandler personoplysninger om ansatte som led i et ansættelsesforhold. Det fremgår videre, at der kun vil være en skævhed, når den registeransvarlige er en offentlig myndighed, hvis den offentlige myndighed som følge af dens relevante offentlige beføjelser kan pålægge en forpligtelse, og samtykket ikke kan skønnes at være afgivet frivilligt under hensyntagen til den registreredes interesser.

KL finder det meget problematisk, at der skabes usikkerhed om, hvorvidt en arbejdsgiver kan behandle oplysninger på grundlag af et samtykke fra den ansatte, ligesom KL finder, at den mulighed, arbejdsgiver i dag har for at indhente fx lægeerklæring og straffeattest med samtykke fra arbejdstageren, skal bevares.

KL finder det endvidere uhensigtsmæssigt, at der skabes uklarhed og tvivl om offentlige myndigheders mulighed for at behandle oplysninger på grundlag af et samtykke fra borgeren, idet bemærkes, at det allerede af artikel 5 fremgår, at personoplysninger skal behandles lovligt og loyalt, ligesom behandlingen skal ske til legitime formål.

KL anbefaler på den baggrund, at det præciseres, at præambel nr. 33 ikke gælder for offentlige myndigheder, samt at præambel nr. 34 udgår. Endvidere anbefaler KL, at der i artikel 7, stk. 4 tilføjes følgende "Dette berører ikke en arbejdsgivers mulighed for at behandle oplysninger på grundlag af et samtykke fra arbejdstageren eller offentlige myndigheders mulighed for at behandle oplysninger på grundlag af et samtykke fra borgeren".

Artikel 8:

KL antager, at "informationssamfundstjenester" defineres på samme måde som i e-handelslovens § 2, stk. 1, nr. 1, som »enhver tjeneste, der har et kommercielt sigte, og som leveres online (ad elektronisk vej over en vis distance) på individuel anmodning fra en tjenestemodtager«. KL har på den baggrund ikke bemærkninger til bestemmelsen.

Såfremt begrebet "informationssamfundstjenester" kan omfatte offentlig information, der ikke har kommercielt sigte, bør det sikres, at eventuelle tjenester i form af anonym rådgivning til børn mv. fortsat kan ske uden tilladelse fra forældrene. En sådan forståelse af begrebet vil desuden indebære meradministration for kommunerne, herunder særskilt behov for at kunne differentiere borgerne på personnumre. Ligeledes vil det betyde meradministration for kommunerne, såfremt kommunerne skal administrere efter særlige EU-blanketter, jf. artikel 8, stk. 4, ved siden af kommunernes nuværende blanketter.

Artikel 9:

KL anbefaler, at det i artikel 9, stk. 2, litra b, præciseres, at behandling er lovlig, hvis den er nødvendig for overholdelsen af arbejdsretlige forpligtelser og specifikke rettigheder i bred forstand, herunder forpligtelser og rettigheder, der følger af kollektive overenskomster mv.

KL anbefaler, at formuleringen af artikel 9, stk. 2, litra f, hvoraf det fremgår, at kun behandling, der er nødvendig for, at et retskrav kan gøres gældende eller forsvares **ved en domstol** ændres, så formuleringen svarer til det gældende direktiv, således at behandling er lovlig, "hvis den er nødvendig for, at et retskrav kan gøres gældende eller forsvares". Således at det bliver tydeligt, at bestemmelsen fortsat omfatter offentlige myndigheders behandling af oplysninger som led i myndighedsudøvelse.

KL anbefaler endvidere, at det i artikel 9 eksplicit præciseres, at arbejdsgivere kan indhente straffeattester.

KL finder, at det bidrager til en problematisk uklar retstilstand, at Kommissionen får adgang til at vedtage delegerede retsakter, jf. artikel 9, stk. 3, med

henblik på nærmere fastlæggelse af undtagelserne fra forbuddet mod behandling af de særligt følsomme oplysninger omfattet af artikel 9, stk. 1, samt kriterierne, betingelserne og de fornødne garantier for behandling af oplysningerne.

Kapitel III Den registreredes rettigheder

Artikel 11: Det er uklart, hvorvidt kravet om, at den registeransvarlige skal "fastsætte regler", jf. artikel 11, stk. 1, indebærer nye administrative forpligtelser for den registeransvarlige.

Artikel 12

KL mener, at kommunerne med artikel 12, stk. 1, pålægges unødig meradministration ved, at kommunerne forpligtes til at udforme diverse procedurer og ordninger for anmodninger om berigtigelse eller sletning og indsigt, herunder pålægges pligt til at udvikle it-understøttelse af borgernes eventuelle anmodninger.

Omkostningerne forbundet med denne meradministration skal ses i lyset af, at de danske kommuner oplever, at borgerne, hvis de ønsker indsigt, anmoder om aktindsigt efter forvaltningsloven og offentlighedsloven. Med andre ord er bestemmelsen på samme måde som den nugældende anmeldelsesordning med til at opbygge et bureaukrati, som ikke kommer borgerne til gode.

Artikel 14 og 15:

Med forslaget til forordning vil den registeransvarlige skulle give borgerne flere oplysninger i forbindelse med opfyldelsen af henholdsvis informationspligt og indsigtsret, herunder bl.a. det tidsrum hvori oplysningerne bevares. Artiklerne er således endnu et eksempel på de øgede administrative opgaver, som forordningen vil pålægge kommunerne.

Kommissionen kan fastlægge standardformularer og angive standardprocedurer bl.a. for den meddelelse, der er omhandlet i artikel 12, stk. 2, for den information den registeransvarlige skal give den registrerede, jf. artikel 14, stk. 8, samt for anmodninger om og meddelelse af indsigtsret, jf. artikel 15, stk. 4. Dette ønsker kommunerne ikke, da det både vil betyde omfattende og dyre justeringer af den IT, der understøtter formularer, procedurer mv. Kommunerne står i dag selv for den nødvendige udvikling af formularer, blanketter mv., hvor alle relevante arbejdsgange som oftest tænkes sammen i én blanket ud fra et effektiviseringshensyn. At skulle administrere, herunder opbevare, journalisere og dokumentere særskilte standardformularer fra Kommissionen vil uden tvivl betyde meradministration for kommunerne. Ligeledes er det tvivlsomt, om borgerne/de registrerede vil opleve det som

en forbedring at modtage flere forskellige blanketter, hvoraf nogle er udarbejdet af Kommissionen.

Artikel 17:
Kommuner og andre offentlige myndigheder er normalt forpligtede til at opbevare sagsoplysninger, for at en sags forløb kan dokumenteres. Det følger derfor af Datatilsynets praksis om sletning af oplysninger hos offentlige myndigheder, at oplysninger hos en kommune som udgangspunkt ikke kan kræves slettet. KL lægger vægt på, at denne praksis kan opretholdes inden for rammerne af artikel 17, stk. 3, litra d, hvoraf det fremgår, at den registeransvarlige ikke skal foretage sletning, hvis det er nødvendigt at bevare oplysningerne for at opfylde en retlig forpligtelse efter EU-retten eller efter medlemsstatslovgivning.

KL finder imidlertid, at det er nødvendigt få præciseret bestemmelsen, herunder navnlig artikel 17, stk. 1, litra b og c, hvorefter personoplysninger skal slettes, såfremt den registrerede tilbagetrækker sit samtykke eller gør indsigelse, samt artikel 17, stk. 4 og stk. 6, således at det sikres, at bestemmelsen ikke er til hinder for, at kommunerne kan opbevare oplysninger med henblik på at kunne dokumentere en sags forløb.

Endelig bemærkes, at kommunernes administrative opgaver øges i forbindelse med krav til sletning efter artikel 17, stk. 3 sammenholdt med præambel nr. 54. KL er sådan set enig i behovet for at udvide sletningsforpligtelsen til også at gælde offentliggjorte oplysninger på nettet. Imidlertid må KL påpege, at også denne bestemmelse er med til at øge kommunernes administrative opgaver. Det samme gælder "begrænsningsforpligtelsen" i stk. 4, samt underretningsforpligtelsen i stk. 6.

Artikel 18: Kravet i artikel 18 om, at kommunerne skal kunne udlevere borgernes egne oplysninger i et særligt format, som den registrerede kan anvende senere, må forventes at kræve omfattende ændringer i eksisterende it-systemer, herunder selvbetjeningssystemer.

Kommissionens ret til ved delegerede retsakter at specificere det elektroniske format og til at fastsætte nærmere regler for videregivelse af personoplysninger, jf. artikel 18, stk. 3, vil desuden indebære, at ændringerne af it-systemerne kan blive særligt omfattende. Det er på den baggrund et forslag, der vil være administrativt meget dyrt og krævende.

Artikel 19: Retten til indsigelse gælder efter det nugældende direktiv ikke, hvis andet er bestemt i den nationale lovgivning, jf. artikel 14 i direktiv 95/46/EF af 24. oktober 1995.

Efter artikel 19 i forslaget til forordning gælder retten til indsigelse mod behandling af oplysninger efter bl.a. artikel 6, stk. 1, litra e, som omhandler behandling, der er henhørende under offentlig myndighedsudøvelse, "medmindre den registeransvarlige påviser vægtige legitime grunde til behandlingen, der tilsidesætter den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder".

Det er efter KL's opfattelse uhensigtsmæssigt, at der med formulering af artikel 19 sammenholdt med præamblen nr. 56, skabes uklarhed om, hvorvidt kommunerne som varetager administrationen af en væsentlig del af lovgivningen af betydning for borgerne, må behandle oplysninger i overensstemmelse med gældende dansk lovgivning, eller om borgerne kan gøre indsigelse efter artikel 19 med den virkning, at kommunerne ikke længere må foretage behandling af de pågældende oplysninger. Der henvises i øvrigt til bemærkningerne til artikel 17 vedrørende offentlige myndigheders dokumentationsforpligtelse.

Artikel 20:

KL finder det uhensigtsmæssigt, at der ikke direkte i forordningen hjemles kommunerne mulighed for at foretage profilering af personer som led i offentlig myndighedsudøvelse. KL lægger i den sammenhæng stor vægt på, at det sikres, at kommunerne også efter en eventuel vedtagelse af forslaget til forordning umiddelbart kan arbejde med profilering i forhold til vurdering af arbejdsstyrken, sundhedsforanstaltninger m.v. På sundheds- og beskæftigelsesområdet arbejdes der eksempelvis med at følge borgere, der er uden for arbejdsmarkedet. Hvis disse borgere bliver syge, hvis de fx. får en psykisk lidelse, regnes der på, hvor lang tid de pågældende borgere gennemsnitligt vil være uden for arbejdsmarkedet, og dermed fx. skal modtage kontanthjælp, i forhold til borgere, der ikke er syge.

KL bemærker desuden, at det er uklart i hvilket omfang artikel 20, stk. 3, udelukker mulighed for at vedtage national lovgivning, der hjemler profilering i forhold til særlige kategorier af personoplysninger.

Artikel 21:

KL vil gerne gøre opmærksom på, at der er flere bestemmelser i persondataloven, der efter KL's opfattelse bør videreføres i national ret, hvis forordningen vedtages, og persondataloven dermed vil blive ændret eller ophævet, bl.a. persondatalovens § 30, stk. 1, om, at underretning til borgeren eventuelt ikke skal ske ud fra en vurdering af hensynet til borgeren selv samt § 30, stk. 2, nr. 6, hvorefter offentlige myndigheders kontrol-, tilsyns- og regule-

ringsopgaver er undtaget fra oplysnings-/underretningspligten. Begge bestemmelser er nødvendige af hensyn til en hensigtsmæssig administration.

KL vil i øvrigt gerne inddrages i og bidrage til det lovgivningsarbejde, i form af ændring af gældende regler i persondataloven med tilhørende bekendtgørelser, forvaltningsloven, sundhedslovgivningen, sociallovgivningen mv., der vil følge med en eventuel vedtagelse af en generel forordning om databeskyttelse.

Kapitel IV Registeransvarlig og registerfører

Artikel 22:

Det fremgår ikke tydeligt af artiklen, hvordan den registeransvarlige skal "påvise", at behandlingen af personoplysninger sker i overensstemmelse med forordningen. Det er uklart, om den registeransvarliges gennemførelse af foranstaltningerne nævnt i stk. 2 er tilstrækkeligt.

KL skal i øvrigt bemærke, at kravet om kontrolmekanismer, jf. artikel 22, stk. 3, er et udgiftsdrivende krav, ligesom det i er øvrigt uklart, hvem der skal udøve det skøn der afgør, om det vil være hensigtsmæssigt at indhente revisorerklæringer.

Artikel 24: KL er enig i behovet for at fastsætte muligheden for delt/fælles dataansvar.

Artikel 28: I artikel 28 indføres nye krav om, at den registeransvarlige og registerføreren skal opbevare dokumentation for "enhver behandling" af personoplysninger, de gennemfører. Bestemmelsen indeholder minimumskrav til, hvilke oplysninger dokumentationen skal indeholde. Denne dokumentation skal stilles til rådighed for tilsynsmyndigheden efter anmodning. KL hilser det velkomment, at anmeldelsespligten, som er indeholdt i det nugældende direktiv 95/46/EF af 24. oktober 1995, ikke videreføres i forslaget til den generelle forordning. KL anser det i den sammenhæng for beklageligt og uhensigtsmæssigt, at Kommissionen indfører nye krav til dokumentationen. Ved at stille sådanne krav til dokumentation for enhver behandling opnås den forenkling, der var formålet med at afskaffe anmeldelsesordningen ikke.

Det fremgår af kravene til dokumentationen, at de som minimum svarer til de krav, der i dag gælder til en anmeldelses indhold. Samtidig udvides dokumentationskravet til at gælde "enhver behandling" I dag gælder alene et krav om anmeldelse af behandlingen af fortrolige oplysninger, jf. persondatalovens § 44, stk. 1.

Set i lyset af at anmeldelsesordningen i dag alene er en bureaukratisk model uden reel værdi for borgerne, der ikke anvender ordningen, er det KL´s vurdering, at der ikke bør stilles nye, unødvendige og bureaukratiske krav til kommunerne om dokumentation.

KL ønsker derfor, at kommuner undtages fra kravet om dokumentation i medfør af artikel 28, stk. 4, alternativt at der som minimum indføres en bagatelgrænse, således at kravet om dokumentation alene gælder, når der sker behandling af følsomme oplysninger omfattet af artikel 9, stk. 1.

Artikel 31:

KL finder, at de omkostninger, der vil være forbundet med en ordning vedrørende anmeldelse af brud på datasikkerheden, ikke står mål med de mulige gevinster, der måtte være forbundet med en sådan ordning. Det forekommer endvidere både urealistisk og uforsvarligt, at der inden for 24 timer skal laves en anmeldelse til tilsynsmyndigheden. Herudover er det efter KL's opfattelse uproportionalt, at der etableres en anmeldelsesordning til tilsynsmyndigheden, som omfatter krænkelse af alle typer af personoplysninger.

KL anbefaler på den baggrund primært, at anmeldelsesordningen og dermed hele artikel 31 udgår af den generelle forordning. Subsidiært anbefaler KL, at artikel 31 ændres således, at forpligtelsen til at foretage anmeldelse til tilsynsmyndigheden kun omfatter tilfælde, hvor der er sket sikkerhedsbrud med hensyn til følsomme oplysninger omfattet af artikel 9, stk. 1.

Artikel 32: KL erklærer sig overordnet enig i, at registrerede skal oplyses om eventuelle sikkerhedsbrud. Imidlertid må KL konstatere, at dette er endnu et eksempel på de øgede administrative opgaver, som forordningen pålægger kommunerne.

Artikel 33:

Efter KL's opfattelse indebærer kravet om, at der skal gennemføres konsekvensanalyser for de behandlinger, der indebærer specifikke risici for den registreredes rettigheder mv. en unødig administrativ byrde.

Uanset at det er forsøgt angivet i artikel 33, stk. 2, er det meget uklart, hvornår der skal gennemføres en konsekvensanalyse. At Kommissionen herudover i medfør af bestemmelsen får mulighed for at udstede delegerede retsakter, bidrager til den uklarhed, der er om, hvad der vil blive gældende ret.

KL har tidligere i den tværoffentlige arbejdsgruppe vedrørende privacy i forbindelse med udarbejdelsen af publikationen: "Retningslinjer til beskyt-

telse af privatlivets fred i tværoffentlige digitaliseringsprojekter", IT- og Telestyrelsen, april 2010 påpeget, at udarbejdelsen af konsekvensanalyser bør være frivilligt. KL's konklusion fra arbejdet i denne arbejdsgruppe var i øvrigt, at de administrative omkostninger forbundet med gennemførelse af konsekvensanalyser ikke stod mål med gevinsterne herved.

KL anbefaler på den baggrund, at bestemmelsen ændres, således at udarbejdelse af konsekvensanalyser bliver frivilligt.

Artikel 35 – 37:

KL er som udgangspunkt enig i, at ansvaret for datasikkerheden skal sikres organisatorisk. KL finder imidlertid, at kommunerne løser opgaven vedrørende sikring af databeskyttelse mv. på hensigtsmæssigt måde inden for rammerne af persondatalovens § 41, stk. 3, og sikkerhedsbekendtgørelsens bestemmelser. KL finder på den baggrund, at forslaget i artikel 35 – 37 er udtryk for en alt for detaljeret regulering af den databeskyttelsesansvarliges stilling og hverv. Hertil kommer, at det databeskyttelsesansvarlige udpeges for en periode på mindst to år og i den periode kan pågældende kun afskediges, hvis vedkommende ikke længere opfylder betingelserne for at varetage hvervet. Dette ser KL som en begrænsning af ledelsesretten, som KL som arbejdsgiverorganisation ikke kan støtte.

KL anbefaler derfor, at principperne i artikel 17 i det nugældende direktiv 95/46/EF af 24. oktober 1995, videreføres for kommunerne, således at det for så vidt angår kommunerne og offentligretlige organer overlades til medlemsstaterne at iværksætte de fornødne tekniske og organisatoriske foranstaltninger vedrørende behandlingssikkerhed.

Kapitel V Videregivelse af personoplysninger til tredjelande eller internationale organisationer

Artikel 44: KL anbefaler, at formuleringen af artikel 44, stk. 1, litra e, hvoraf det fremgår, at videregivelse kan ske, hvis videregivelsen er nødvendig for, at et retskrav kan gøres gældende eller forsvares **ved en domstol** ændres til "videregivelsen er nødvendig for, at et retskrav kan gøres gældende eller forsvares". Der henvises til KL's bemærkninger til artikel 9, stk. 2, litra f.

Kapitel VIII – Klageadgang, ansvar og sanktioner

Artiklerne 78 – 79:

Efter KL's vurdering vil der ifølge bestemmelserne kunne udstedes bøder til kommunerne, som er uforholdsmæssigt høje i forhold til forseelsernes karakter, herunder fx bøder på 250.000 EUR (1.875.000 kr.) for manglende eller mangelfuld overholdelse af den registreredes rettigheder og bøder på 1.000.000 EUR (7.500.000 kr.), hvis der ikke udpeges en databeskyttelsesansvarlig.

Ligeledes vurderer KL, at det høje bødeniveau vil være helt ude af trit med den måde kommunernes administration normalt plejer at blive sanktioneret, hvor pålæg og henstillinger plejer at være tilstrækkeligt. KL ønsker derfor, at bøderne ikke skal gælde for kommunerne, alternativt at bødeniveauet i forslaget til forordning generelt sættes ned for offentlige myndigheder.

Kapitel IX – Bestemmelser vedrørende specifikke databehandlingssituationer

Artikel 81: Af artikel 81, stk. 3, fremgår det, at der skal stilles "garantier" i forbindelse med behandlingen af sundhedsoplysninger. De administrative krav og konsekvenser i forhold til disse garantier fremgår ikke klart.

Artikel 82

I Danmark er arbejdsgivers behandling af persondata ikke underlagt specifik arbejdsretlig lovgivning, men er i det væsentlige baseret på kollektive aftaler, ledelsesretten og samarbejdsudvalgssystemet.

Der er i dag mulighed for ved kollektiv aftale at vedtage en mere vidtgående beskyttelse af personoplysninger. Arbejdsmarkedets parter har fx aftalt krav om længere varsling ved iværksættelse af kontrolforanstaltninger end de krav, der fremgår af det gældende databeskyttelsesdirektiv.

Forordningen giver mulighed for at "vedtage specifikke bestemmelser" for behandling af persondata i ansættelsesforhold "under overholdelse af denne forordning" , men det er nødvendigt, at det i forordningens artikel 82 præciseres, at dette også kan ske via kollektive overenskomster.

Det anbefales på den baggrund, at formuleringen i artikel 82, stk. 1, ændres til "Under overholdelse af denne forordnings artikel 5 kan medlemsstaterne vedtage specifikke bestemmelser ved lov eller ved kollektive aftaler, der regulerer behandlingen.....".

Artikel 83

KL er imod forslaget til artikel 83, da forslaget ikke tager højde for arkivlovens bestemmelser, herunder bl.a. arkivlovens 75 års regel.

Dette kombineret med, at Kommissionen har mulighed for at vedtage delegerede retsakter, jf. artikel 83, stk. 3, vil indebære, at Kommissionen vil kunne vedtage retsakter, der bl.a. erstatter arkivlovens 75 års regel samt indsigtsregler, der er mere vidtgående end de gældende danske arkivregler giver mulighed for.

Kapitel X - Delegerede retsakter og gennemførelsesforanstaltninger

Artikel 86: KL finder, at den adgang, Kommissionen ifølge forslaget til forordning får til at udstede retsakter, hvor Kommissionen fastlægger kriterier og betingelser i forhold til de enkelte bestemmelser i forordningen begrænser det nationale råderum, ligesom det giver en høj grad af usikkerhed om, hvad der er og bliver gældende ret. Der henvises i øvrigt til KL's bemærkninger i det generelle høringssvar, samt til KL's bemærkninger til de enkelte artikler.

Justitsministeriet
jm@jm.dk

28. juni 2012

Dok. 126797/ah

Høringssvar om EU-Kommissionens forslag om nye databeskyttelsesregler

Med henvisning til Justitsministeriets brev af 11. maj 2012 (j.nr. 2012-3756-0005), skal Forbrugerrådet hermed afgive sine bemærkninger til forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) (KOM (2012) 11 endelig).

Forbrugerrådet hilser Kommissionens ambitiøse forslag af 25. januar 2012 om at reformere de eksisterende databeskyttelsesregler velkommen. Vi finder, at forslaget på én gang styrker forbrugernes digitale rettigheder og sikrer virksomhederne ensartede regler. Harmoniseringen kan skabe den nødvendige tillid til, at fordelene ved den teknologiske udvikling, som effektivisering og vækst i digitale tjenester og produkter, høstes fremadrettet.

Forordningen er nødvendig, da de eksisterende regler er forældede i forhold udviklingen, og derfor ikke længere yder forbrugerne en tilstrækkelig beskyttelse. Siden de nuværende regler om beskyttelse af personoplysninger blev vedtaget i 1995, er der sket en kolossal vækst i den teknologiske udvikling til fordel for både forbrugere, virksomheder og samfundet generelt. Men digitaliseringen har samtidig betydet nye udfordringer i forhold til at sikre den enkeltes ret til respekt for sit privatliv. Det skyldes, at personlige oplysninger indsamles og anvendes af private og offentlige virksomheder i et hidtil uset omfang. Oplysningerne indsamles typisk som en betingelse for at opnå en bestemt service eller gøre brug af en tjeneste eller et produkt, ligesom vores onlineadfærd registreres og anvendes i kommerciel henseende. Ikke mindst i offentlige virksomheder indsamles følsomme oplysninger i dag digitalt.

Den omfattende dataindsamling har forringet forbrugerens kontrol med egne oplysninger og kan, hvis ikke databeskyttelsesreglerne moderniseres væsentligt, på sigt føre til, at forbrugernes tillid til de digitale tjenester svækkes. Det vil i givet fald betyde, at man ikke kan opnå gevinsterne ved den digitale udvikling.

Uanset at de danske forbrugere er kendt for deres høje tillid til offentlige og private virksomheder, viser seneste europæiske forbrugerundersøgelse, at 61 % af den danske befolkning ikke har tillid til, at internetvirksomheder, som søgemaskiner og

Fiolstræde 17
Postboks 2188
DK-1017 København K

Tlf. (+45) 7741 7741
Fax (+45) 7741 7742
Mail fbr@fbr.dk
Web www.fbr.dk

sociale netværk, kan beskytte deres personlige information. Tallet på EU-plan er 62 % (jf. Eurobarometer 359/2011). Samtidig er der ifølge kriminolog og forsker i identitetstyveri Peter Kruize fra Københavns Universitet sket en fordobling i antallet af identitetstyverier herhjemme fra 2009 til 2011.

Derfor er det vigtigt, at de kommende databeskyttelsesregler både kan øge tilliden til det digitale marked og beskytte forbrugernes privatliv mod fx identitetstyveri. Forordningen skal således dels sikre forbrugerne nogle nye rettigheder, som tager højde for den digitale tidsalder, dels øge de tekniske krav til offentlige og private virksomheders it-systemers håndtering af personoplysninger, og endelig er det afgørende, at reglerne understøtter et effektivt tilsyn.

Forbrugerrådet vil gerne fremhæve følgende områder, som vi finder, er særlige vigtige at få indarbejdet i databeskyttelsesforordningen:

1. Opstramning af samtykke-kravene

Retten til selv at bestemme, om ens personlige oplysninger må indsamles eller ej, er fundamental for forbrugeren, både i den analoge og i den digitale verden. Digitaliseringen og virksomhedernes øgede interesse i at indhente personlige oplysninger har imidlertid gjort samtykke-beskyttelsen illusorisk i praksis. Det skyldes, at forbrugeren i dag "tvinges" til at afgive bestemte oplysninger, som fx CPR-nummeret, som betingelse for at opnå en bestemt tjeneste, service eller for at tage et produkt i brug.

Forbrugerrådet er derfor tilfreds med Kommissionens forslag om at stramme samtykkereglen i forhold til bevisbyrde og tilbagekaldelse. Vi finder, at det er særdeles vigtigt, som foreslået, at få indført en regel om, at et samtykke ikke generelt er tilstrækkeligt til, at virksomhederne kan tilsidesætte enhver databeskyttelse, og at samtykket er ugyldigt, hvis der er en klar skævhed mellem parterne. Forbrugerrådet oplever en uheldig tendens til, at virksomheder i stigende omfang opretter såkaldte positive registre, hvor kunde-data på samtlige brugere registreres og udnyttes kommercielt, selv om de objektive behov måske kun tilsiger registrering af et fåtal.

Derimod kan Forbrugerrådet ikke støtte, at forslaget tilsyneladende ikke forhindrer, at virksomheder kan indhente samtykke til flere formål på én gang. Denne mulighed har skabt grobund for et marked for videresalg af samtykker og uigennemsigtige abonnementsaftaler, som maskeres som online-konkurrencer. Desuden er det uklart, hvorvidt det nuværende forbud mod at videregive oplysninger til brug for markedsføring bortfalder. En sådan svækkelse af forbrugerens retsstilling, kan Forbrugerrådet ikke støtte, set i lyset af den høje værdi salg af kundeoplysninger har fået.

2. Anvendelse af privatlivsbeskyttende teknologi

Forbrugerrådet støtter kommissionens forslag om, at virksomheder, som behandler risikofyldt data, skal foretage en konsekvensanalyse inden dataindsamlingen påbegyndes.

Som konsekvens af den omfattende digitale behandling af personoplysninger i offentlige og private virksomheder, finder Forbrugerrådet især, at forslaget om, at virksomheder skal indbygge databeskyttelse i deres it-systemer fra start af, er uhyre vigtigt. Det kan fx ske ved at fjerne kunde-ID'er i databaser og i stedet anvende pseudonymisering, så risikoen for datalæk eller hacking minimeres (jf. konkrete eksempler på Privacy by Design løsninger i digitaliseringsstyrelsens oplæg "Diskussionspapir om nye digitale sikkerhedsmodeller", januar 2011).

Der er således behov for at få opdateret databeskyttelsesreglerne, så de fremtidssikres i forhold til den videre teknologiske udvikling. Ved at øge fokus på teknisk sikkerhed, kan data anvendes til gavn for virksomheder og forbrugere – og ikke på bekostning af den enkeltes ret til respekt for sit privatliv.

3. Forbud mod profilering og retten til at flytte data og blive glemt

Sociale medier og søgemaskiner har en stigende popularitet og udbredelse. Men de skaber nye udfordringer i relation til den enkeltes kontrol med egne oplysninger, både i relation til oplysninger, man selv og andre deler, og de data udbyderen indsamler om brugerens bevægelser på tværs af nettet. Omfanget af oplysninger, som registres over tid, er enormt, og det er svært at gennemskue, hvor ens oplysningerne havner, hvem der har adgang til dem og hvad de kan blive brugt til på sigt.

Forbrugerrådet støtter derfor bestemmelserne om, at forbrugerne dels skal kunne flytte alle oplysninger fra én udbyder til en anden, dels kan kræve, at udbyderen sletter allerede registeret data og undlader yderligere spredning af personoplysninger. Endelig støtter Forbrugerrådet forslaget om at forbyde automatisk profilering om en persons erhvervsevne, økonomi, lokalitet, sundhed, pålidelighed eller adfærd.

4. Effektivt tilsyn og øget sanktioner

Forbrugerrådet savner generelt for området, at forbrugerens interesser varetages af en proaktiv og debatskabende instans, en uafhængig vagthund, som dels kunne informere forbrugerne om deres rettigheder, dels kunne rådgive virksomhederne om at etablere privatlivsvenlige it-løsninger, som rækker udover eksisterende lovgivning.

Forbrugerrådet hilser derfor forslaget om at styrke EU-datatilsynenes uafhængighed og ressourcer velkommen. Desuden finder vi, at forslagene om et europæisk databeskyttelsesråd, udpegning af databeskyttelsesansvarlige i virksomheder, anmeldelsespligten ved databrud samt forslaget om administrative, høje sanktioner, er helt afgørende for at sikre forbrugerne en tilstrækkelig privatlivsbeskyttelse fremover.

Se Forbrugerrådets specifikke bemærkninger i BEUC's "draft position paper" (vedlagt)

Den europæiske forbrugerorganisation BEUC har udarbejdet et detaljeret udkast til høringssvar til EU Kommissionens forslag til persondataforordningen på baggrund af input fra ca. 40 medlemsorganisationer. Dette vedlægges, idet Forbrugerrådet

støtter indholdet til fulde (en oversættelse til dansk eftersendes, når BEUC's endelige svar foreligger).

Da det endnu ikke er helt klart, hvilke konsekvenser reguleringsformen får i en dansk kontekst, vender vi gerne tilbage med flere bemærkninger senere.

Med venlig hilsen

Vagn Jelsøe	Anette Høyrup
Afdelingschef	Seniorrådgiver, Cand.jur.

Draft Regulation on Data Protection

BEUC Draft Position Paper

Summary

(To be completed at the end)

The European Consumers' Organisation (BEUC) welcomes the European Commission's proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Overall, the draft Regulation addresses the main challenges and the shortcomings of the current Framework with the aim of enhancing the rights of data subjects and restoring control over the processing of their own personal data, especially in light of the constantly evolving ICT developments. The EU needs to have a consolidated general framework that will apply across the board, which could then be complemented by more specific rules if necessary.

The revision of the current Framework also acknowledges the changes brought by the Lisbon Treaty. In fact, both the European Charter of Fundamental Rights and the European Convention on Human Rights which recognize the fundamental rights to the protection of personal data and to privacy - will now need to be fully complied with by both the EU institutions and Member States, acting within the scope of the EU law.

Although the proposal overall constitutes a major improvement for individuals, a number of provisions still need to be clarified or modified to ensure that the EU new framework is effective and becomes the global standard in the field of protection of personal data and privacy.

CHAPTER I – General provisions

Article 2 – Material scope

Article 2 of the proposal defines the material scope of the regulation in the same terms as directive 95/46: it applies to the processing of personal data wholly or partly by automated means or to the processing of non automatic means of personal data which forms part or is tended to form part of a filling system.

However, the exceptions to the general scope are more developed in the proposal than in the current Directive. While we do not oppose the exceptions we think that they should be better defined to avoid different interpretations and undue use of personal data in borderline cases.

Regarding the exception of **national security**, we would like to highlight that the scope of this notion often differs from one Member State to another, which will undermine the uniform application. Thus, we think that the Regulation should introduce certain criteria that better defines the extent of this exception.

With regard to the exception of **personal and household activities**, we welcome the reference to the gainful interest as the main criterion for the application of the exception. The question of whether individuals processing data for personal and household activities is particularly important within a technological context, with individuals posting content online through social networking sites, blogging sites etc. We would however recommend including in Article 2 the elements of the definition of

"gainful interest" provided in recital 15, namely that the notion is linked to professional or commercial activity.

Furthermore, the draft Regulation does not clarify the application of the exception when data is made available to an indefinite number of individuals. According to the case-law of the European Court of Justice[1], the exception should only apply when the data is made available to a limited number of individuals. We would therefore suggest that the exception of Article 2.2.d be complemented with the criterion of indefinite number of people, thus clarifying that an indefinite number of contacts shall in principle mean that the household exception does no longer apply.

Article 3 – Territorial scope

Article 3 deals with the territorial scope of the proposal, addressing the case of the data controller being established within the European Union and outside the European Union.

Article 3.1, introduces the criterion of **establishment in the EU** to determine whether EU law would apply. However, the definition of the establishment, as the place where the main decisions as to the purposes, conditions and means of processing are taken (Article 4.13) is not appropriate for undertakings with decentralized decision making structure, where the central administration and the place where management decision about data processing are made differ.

Furthermore, Article 3.1 only provides for the application of EU law without any criteria to determine which national law shall apply. This is in principle logical as the Regulation is supposed to be a self-standing instrument. However, the Regulation leaves some scope for the application of national law in some of its provisions and Member States maintain the freedom to adopt specific legislation in a limited number of areas. The draft Regulation only provides for criteria to define the leading Data Protection Authority (Article 51) where several Member States are concerned, but does not address the issue of national applicable law.

Article 3.2 refers to cases where the data controller is **not established in the EU**, but the processing activities are related to the offering of goods and services to data subjects residing in the EU or monitoring of their behavior. Compared to article 3 of the current directive, this new provision takes away the criterion of 'use of equipment".

Although BEUC welcomes the new criteria, further clarification is needed to ensure that the offering of goods and services also includes the so-called those services the which are based on monetizing the secondary use of consumers' data[2].

Article 4 – Definitions

- Article 4.1- Definition of "data subject" (personal data)

[1] See ECJ 6 November 2003, Lindquist and Satamedia, C-101/0.
[2] Opinion 01/2012 on the data protection reform proposals by Article 29 Data Protection Working Party.

Compared to the present Directive, in the new proposal the criteria for the definition of "personal data" are transferred to the definition of "data subject". The main elements of the definitions remain in place, which BEUC welcomes. We think that the broad definition in the proposal provides the necessary flexibility to be applied to different situations and developments affecting the fundamental right of privacy and data protection in the light of rapid ICT developments[3].

In particular BEUC welcomes that the new proposal widens the definition by including the concepts of on line identifiers and location data. However, the proposed new definition contrasts with the wording in the last sentence of recital 24[4]. This sentence undermines the aim of the new definition which is to cover any information or means that allows the identification of a data subject. As soon as the information allows the data controller to identify an individual, the information should be deemed personal data. BEUC thus considers that the last sentence of recital 24 should be redrafted clarifying that **when there is a close relation between the identified and an individual** this will trigger the application of data protection rules.

BEUC would caution against overstretching the application of data protection rules to every single situation when information if processed, but its application should depend on the specific context and on whether the information processed can be linked to a specific person.

The application of the proposal's definition in specific cases should also reflect the primary objective of the draft Regulation which is the protection of the fundamental right to protection of personal data. BEUC would be opposed to a narrow definition that would leave individuals deprived of any protection.

- Article 4.8- Data subject's consent

The draft Regulation establishes data subject's consent as one of the possible grounds for legitimizing data processing, both for personal and sensitive personal data. Article 4.8 requires consent to be freely given, specific, informed and explicit, while Article 7 establishes a number of conditions for consent, including the burden of proof on the controller to demonstrate that the consent requirements are met.

BEUC welcomes the provision in recital 25 that consent can be given by "any appropriate method", which allows for a certain degree of flexibility, provided that it transparent and meaningful, as well as the provision that the request to give consent in the online environment should not be disruptive to the use of the service and should hinder the data subject' online experience.
BEUC recognises that there is no 'one size fits all' solution to the issue of consent, while the means of implementation of consent of consumers should be flexible and user-friendly. We believe that practices could be assessed against the two following criteria:

- An analysis of the potential consumer detriment linked to a specific practice/ technique.

[3] The proposal follows the recommendations of the opinion of the 29 data protection Working Party: Opinion 7/2007 of 20 June 2007.
[4] Recital 24: "...identification numbers, location data, on line identifiers...need not necessarily be considered as personal data in all circumstances".

- An evaluation of whether a practice/technique meets the 'reasonable expectations' of uses of their information by an average or typical consumer or by the average member of the group when it is directed to a particular group of consumers.

BEUC would therefore suggest focusing on the requirement for consent to be meaningful, while it needs to be clearly stated that consent is only one of the legal grounds for processing and not necessarily the most appropriate one in all circumstances. For example, consent cannot be valid when the requirements of transparency and information have not been met. Most importantly, compliance with the principles for data protection processing, including data minimization and purpose limitation needs to be ensured.

- Article 4.13- Main establishment

The main establishment is defined as the place where the main decisions as to the purposes, conditions and means of processing are taken. However, this definition is not appropriate for undertakings with decentralized decision making structure, where the central administration and the place where management decision about data processing are made differ. For those cases, the main establishment of the group may be used as the determining factor, or alternatively the dominant influent of one establishment over the others.

- Article 4.20 (new)- Transfer of personal data

BEUC regrets that the draft proposal does not provide for a definition of what is to be considered as a transfer of personal data. The main question arises in relation to the passing of data between companies in the same countries and other types of exchanges on networks, such as servers of companies. In a number of Member States, such transfers are prohibited and therefore the omission of this rule from the draft Regulation would result in significant decrease of consumer protection.

CHAPTER II – Principles and lawfulness for processing

Chapter II of the proposal deals with the principles of data processing and adds specific requirements to apply to the collection and processing of data related to minors and of sensitive data. BEUC welcomes that the general principles of data processing are maintained in the proposal while significant improvements are put forward in particular as regards the principle of transparency.

Article 5 – Principles relating to personal data processing

BEUC welcomes the introduction of the **principle of transparency** in relation to the collection and processing of data. This reflects the stronger obligations put on the controller to inform data subjects (article 14 of the proposal) about the most relevant information regarding the processing, including the identify and the contact details of the controller, the purposes of the processing, the retention period, the existence of rights and the modalities to exercise them etc, as defined in Article 14. Lack of transparency and information is a major deterrent to users in the assertion of their rights. If they do not know how their data is being used, for what purpose and by whom, they will not be in a position to exercise and enforce their rights.

The proposal enhances the principle of **data minimisation** by giving it more visibility in a new paragraph (e). The strengthening of this principle is necessary in order to address the current trends of data harvesting and data mining used for profiling consumers which involve large amounts of personal data being collected. Many data controllers retain data beyond the necessary time to perform the service. In the specific case of search engines, the article 29 Working Party required search engine providers "to delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times".

The principle of data minimization also mirrors the new principles of privacy by design and privacy by default according to which data protection principles need to be embedded in privacy-sensitive technologies and services, right from the beginning of their development.

The principle of **purpose limitation** of data processing is of utmost importance in relation to the proliferation of business models that are construed on the basis of data sharing with third parties. The business models of many Internet companies (e.g. some search engines, social networking sites...) are often incompatible with the principle of purpose limitation and the specification of use of personal data. Many companies collecting personal data transmit the data to third parties that process these data for different purposes from those initially pursued by the data controller often without informing the data subject.

BEUC **regrets** that the concept of "compatibility" (with the original purpose of processing) is not defined in the proposal. The criteria of "compatibility" due to its vagueness (without specification of what is compatible or incompatible), has brought about divergences at national level . In a few countries the principle is defined in excessively broad terms undermining the very principle. In this regard, we think that the new regulation should include some criteria as to what is considered "compatible", drawing on best practices of the way "compatibility" has been interpreted at national level .

Article 6 – Lawfulness of processing

Article 6 of the proposal reproduces the grounds for processing present in the current Directive. The processing of personal data is lawful when at least one of the following applies:

a) the data subject has given its consent to the processing,
b) processing is necessary for the performance of a contract,
c) processing is necessary for compliance with a legal obligation,
d) processing is necessary to protect the vital interests of the data subject,
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of a public authority vested on the controller,
f) processing is necessary for the purposes of the legitimate interest of the data controller unless such interest contrast with the fundamental rights and freedoms of the data subject.

Compared to the existing directive, the proposal contains a few but very important novelties. The most welcome changes relate to the definition and the conditions for "consent" (article 7) as well as the provision on the processing of personal data of a child (article 8).

When processing is based either on controller's compliance with a legal obligation or on the public interest, the basis for the processing will have to be provided either in EU law or the national law of a Member State (Article 6.3). This provision is very important as it excludes the law of a non -EU country as the legal basis, as would be the case where processing of personal data of EU residents may be required for law enforcement purposes by third countries.

BEUC is concerned that unless properly defined, the general notion of **"legitimate interests** of the controller" might open the door to abusive processing. According to paragraph 5 of article 6, the Commission is empowered to adopt delegated acts to further specify the conditions for processing based on the legitimate interests of the data controller. BEUC considers that delegated acts are not the appropriate means to address the boundaries of the legitimate interests of the data controller as there is a risk of surpassing the legal grounds; on the contrary the regulation should included some rules on the boundaries of the legitimate interests of the controller.

Article 7 – Conditions for consent

The draft Regulation establishes data subject's consent as one of the possible grounds for legitimizing data processing, both for personal and sensitive personal data. Article 7 establishes a number of conditions for consent, including the burden of proof on the controller to demonstrate that the consent requirements are met.

BEUC welcomes the provision in recital 25 that consent can be given by any appropriate method, which allows for a certain degree of flexibility, as well as the provision that the request to give consent in the online environment should not be disruptive to the use of the service and should hinder the data subject' online experience of the service. As stated above, there is no 'one size fits all' solution to the issue of consent, while the means of implementation of consent should be flexible, user-friendly and ensure meaningful consent.

We are satisfied that article 7 puts the burden of proof of the consent on the controller. Thus the controller should pay special attention to the reliability of the means used to obtain consent of the data subject in accordance with recital 25.

We also welcome the inclusion of the right to withdraw consent at any time which is wider than the "right to object" in the current directive.

However, for consent to be valid, the conditions of informed, specific and free will have to be met. The draft regulation provides examples of cases where consent cannot be valid due to a lack of balance between the parties, for instance in the employment sector. We highlight however that the lack of balance is present also in other sectors such as the insurance sector – where often the benefit of special conditions as tied to the consent of the consumer to the processing of his/her data; recital 34 should thus add the insurance sector as an example of possible lack of balance. As regards the "informed" consent, the data subject should receive clear and understandable information (in a concise manner) on key elements that are defined in Article 14.

Article 8 - Processing of personal data of a child

BEUC welcomes the new provision in article 8 that requires parental consent for the processing of personal data of a child.

In particular in the on line environment minors do not always have the knowledge to realize the consequences of the collection/processing of their personal data. Internet and new technologies offer ever wider possibilities to children to share data (photos, videos, messages, localization information through blogs, videos, social networks...) which combined with the lack of awareness of the risks and dangers of data collecting, make children and teenagers the most vulnerable group in the digital world.

However, we see a number of problems regarding the implementation of the obligation of parental consent. First, the threshold of 13 years old might conflict with national laws relating to the legal capacity to conclude a contract, the processing of data occurring very often in the context of a contractual relationship. Second, the obligation to develop means to verify the legitimacy of parental consent, should not lead to further processing of data which otherwise would not be necessary to process. We also think that the criteria and modalities for the parental consent should not be totally left to delegated acts of the Commission; some criteria should be included in the regulation itself.

In addition this provision seems to apply only in the context of the "offering of information society services". The meaning of offering information society services seems to be too restrictive and it should be clarified; the provision should apply to any processing of personal data of a child both on and off-line.

Article 9 - Processing of special categories of personal data

We welcome the prohibition of collection/processing of sensitive data as referred to in article 9.1 of the proposal. BEUC believes that the list of sensitive personal data must be exhaustive to ensure legal certainty and avoid divergent implementation at national level. We consider however that also financial data should be added to the list of Article 9.2 when revealing personal solvency. Other financial data such as the unpaid debts of clients to the company with which it is or has been in a contractual relationship would not make part of this category.

Finally, we believe that the specificities, conditions and safeguards for the processing of sensitive data should not be left to delegated acts of the Commission; sensitive data requires an additional layer of protection and thus the conditions for their processing need to be clarified in the regulation. Alternatively, this could be the object of opinions/reports of the European Data Protection Board.

CHAPTER III – Rights of the data subject

Article 11 – Transparent information and communication

Lack of transparency and lack of clear information is a major deterrent to users in the assertion of their rights. Consumers rarely understand privacy notices which are generally too lengthy. According to different surveys although consumers are concerned about their privacy, they do not view privacy policies as a suitable way to understand and answer their privacy concerns. These findings are confirmed by behavioural economics considerations, which show that consumers do not read privacy notices and are prone to accept default settings.

The proposal significantly strengthens the information obligations of the controller to the data subject (articles 11, 12 and 13). We in particular welcome the new requirement that information has to be provided in an intelligible form and using clear and plain language. We also support the regulation of procedures for providing the information to the data subjects as this will strengthen accountability of the controller vis-à-vis the data subject.

Article 12 – Procedures and mechanisms for exercising the rights of the data subject

BEUC welcomes the introduction of specific modalities for the exercise of the rights of the data subject. Data controllers should respond to request by data subjects without undue delay and no later than one month. Furthermore, data controllers should not be able to charge for a data subject's access to his own personal data, as long as this right is not abused. As regards the right to correct, erase and delete data, it should always remain free of charge, as it is also to the benefit of the data controller to have correct and updated data.

Article 13 – Rights in relation to recipients

BEUC welcomes the introduction of an obligation for the data controller to notify each recipient to whom data has been disclosed in case of rectification or erasure, as long as it is possible without a disproportionate effort. This provision is particularly important in the online environment, where data can easily be shared with third parties and therefore inaccuracies need to be corrected.

Article 14 - Information to the data subject

Article 14 sets up a list of all the information the data controller is obliged to give to the data subject in case of collecting/processing of his personal data. Overall this provision is comprehensive of the relevant information the data subject needs to have. However, information about the type of personal data collected and processed is currently missing from the list and should be added.

We welcome the new obligation of the data controller to inform the data subject of his right to lodge a complaint to the supervisory authority and his contact details, reflecting the new right of the data subject to directly lodge complaints (article 15.1 (f)). However, data subjects also need to know about the procedures to lodge such complaints; this should be added to the text; often consumers are not aware of the procedural steps in order to lodge complaints.

In addition, this provision should echo the inclusion of a specific article dealing with profiling (article 20) by adding a reference to profiling purposes and its consequences on individuals, in article 14.1 b.

Regarding the exceptions to the information obligations listed in article 14.5, we think that the exception in article 14.5 b) (when the information to the data subjects proves impossible or carries a disproportionate effort) should be better defined in the regulation, instead of letting the Commission adopt delegated acts to specify such exception.

It is important to inform the data subject which personal data is obligatory to provide and which is voluntary. As regards services whose business model is based on monetizing the use of consumers' personal data in exchange for so-called "free services", it should be made crystal clear to the consumer that this exchange is taking, while the processing of data should comply with the general principles of data minimization, purpose limitation etc.

We support the reference to standard forms to lay out the information provided to the data subject but we think that this should be a requisite rather than an option; Standard forms generally offer better and more structured information to the consumer. We also think that the new European Data Protection Board (EDPB) should take the lead in developing such standard privacy notices with the participation of consumers' representatives and businesses.

Finally, the possibility for data controllers to present the information by using multilayered notices should be expressly allowed.

Article 15 - Right of access for the data subject

Article 15 includes a list of information obligations in relation to the right of the data subject to access the data processed at any time. Compared to the current directive, the addition of the obligation to inform about the right to lodge a complaint to the supervisory authority and its contact details (15.1 (f)) is very welcome. Yet, as said above, data subjects should also be informed about the procedures to lodge complaints. Consumers cannot fully benefit from their rights if they are not informed about the ways to complaint and to obtain redress in case of infringement.

Article 17 - Right to be forgotten and to erasure

The digital print left by individuals when personal data is processed on line is problematic for consumers; consumers may well wish to erase the traces they leave behind on the Web at one point in time .

BEUC supports the intention of the "Right to be forgotten" which aims to strengthen the right to erase personal data. Even though the right of erasure is included in the current directive, its application in the on line environment is very often ignored: various studies and surveys have reported the difficulties data subjects have in exercising such right .

The new article 17 should allow a better enforcement of the existing right of erasure in the digital environment; indeed, according to the new proposal the controller will be held liable in case he has made the personal data public or has authorised the processing of the data by third parties.

However, we consider that the naming ("forgotten") is misleading as the limitations of a "right to be forgotten" are manifold and have to be acknowledged. . An unconditional right to be "forgotten" may raise concerns regarding its compatibility with freedom of expression and information while its implementation and enforcement must not result in the application of technical measures resulting in the filtering of online communications. The relationship with the provisions of the e-commerce Directive on the liability of information service providers needs to be carefully assessed.

Moreover, in many cases it would be impossible to inform all parties to whom data has been disclosed and track down all possible links and copies of data. In this regard, article 17.2 should make it clear that only an obligation of effort is imposed on the controller and not an obligation of result.

Finally, the requirements, conditions and criteria for the implementation of the right to be forgotten should not be left to delegated acts of the Commission but should be defined in the regulation.

Article 18 - Right to data portability

BEUC very much welcomes the introduction of the new right to data portability in the proposal (article 18). In the on line environment consumers store huge amounts of information (e.g. social networks, e-mail services...).. At present too often consumers are locked-in to online services and platforms with no possibility of transferring these data onto other (competing) platforms. Existing terms and services appear mostly to be unfair in this regard: often service providers claim ownership of the data stored in their services.

This situation is incompatible with the right of consumers to be in control of their data and to object to the processing of their data. It also hinders competition among service providers and prevents switching. The right to data portability allows the consumer to be in control of his data and retain the ownership, by being able to shift the data to other services.

The relationship between the right to data portability and the right of erasure should be better clarified in the proposal. It should be clearly established that the right to data portability implies the erasure of the data by the original service provider (the use of the word "copy" in article 18.1 seems to imply that the original service provider can retain the data and only give away a copy). In any case the data controller is always obliged to delete the data when they are no longer necessary for the purpose for which they were processed (article 5 e)).

However, an effective implementation of the right to data portability necessitates the development of interoperable or compatible standards which need to be developed.

Article 19- Right to object

Article 19 of the proposal establishes the right to object of the data subject to the Article 19 of the proposal establishes the right to object of the data subject to the processing of his data, collected on certain grounds, unless the controller demonstrates compelling legitimate grounds for the processing. There is a significant

improvement from the current situation, where the data subject only has a right to prevent processing where he/she can demonstrate damage is caused. According to Article 19, the data subject will have by default a right to object to processing and it will be for the data controller to demonstrate why the objection is not valid and to justify the processing.

This provision however, does not make clear the consequences of the right to object in the relation to the data at stake. It should be clarified that the right to object, if upheld by the controller should result in the deletion of the data by the controller.

Moreover, the notion of "compelling legitimate grounds" which (despite the objection) could legitimise the processing, should be developed in the regulation.

Article 20 - Measures based on profiling

Article 20 addresses the processing of personal data for the purposes of profiling individuals according to their personal aspects, preferences and behaviour. Advertising business models using profiles of individuals are proliferating and consumers are often not aware of these practices or of the consequences of such practices in the economic decisions they take. Consumers have almost no control over the current complex "media and marketing ecosystem".

Therefore, BEUC welcomes the specific inclusion of profiling practices in the proposed regulation. BEUC is not inherently opposed to the tracking and profiling of consumers on-line. In this logic, the draft regulation does not prohibit profiling but indeed gives the right to the consumer to object to profiling.

However, in order to ensure legal certainty it must be clarified what is meant by "legal effects" and "significantly affects". Moreover, the right to object should be accompanied by the right to be informed about the techniques and procedures used for profiling in the advertising ecosystem ; this obligation already exists in the current directive and it should be reintroduced in the proposal. Equally, consumers should be informed of the possible consequences of profiling techniques applied to them.

The draft proposal should also prohibit profiling of vulnerable consumers such as children as those consumers often lack critical judgment and understanding of marketing techniques; those techniques could have a negative impact on children and young people's cognitive and emotional development.

Regarding paragraph 5, we do not support the reliance on delegated acts to specify the safeguards to protect the consumers' legitimate interests in case of profiling. On the contrary, the safeguarding measures should be defined in the regulation.

Article 21 - Restrictions

Article 21 of the proposal introduces a number of possible restrictions to the rights of data subjects. We notice that this article is much wider than the corresponding article in the current Directive (article 13). Contrary to the current Directive, the new article 21 can be used to limit almost all the rights of the data subject (including the

principles of processing, the right to object, measures based on profiling and the right to be notified of a data breach).

We consider that article 21 should include certain guaranties in relation to the purposes, proportionality and necessity of the processing, the categories of data collected and the persons authorized to process the data. There is a need to define with more clarity the specific guarantees that the law allowing such restrictions should establish to safeguard the legitimate interests of the data subject.

CHAPTER IV – Controller and Processor

Article 22- Responsibility of the controller

The Draft Regulation introduces the principle of accountability, according to which the data controller must put in place measures and control systems that ensure compliance and provide evidence to demonstrate compliance to external stakeholders, including supervisory authorities.

Article 22 introduces a general obligation for the controller to implement appropriate and demonstrate compliance while the following articles of Chapter IV introduce further elements of accountability, including the carrying of Data Protection Impact Assessment, the appointment of Data Protection Officer, the implementation of Data Protection by design and by default and the obligation to notify data breaches.

BEUC welcomes the new provisions that will enhance controller's responsibility and help create a privacy and data protection culture within companies. They will also allow controllers to adopt the measures that are the most appropriate for the nature of their processing operations, thus providing a high degree of flexibility that is required within a fast-evolving technological context.

In addition to the requirement to demonstrate compliance to the DPA, it is equally important that controller demonstrates compliance to the public in general by means of an annual report describing the measures adopted.

The principle of accountability should not be perceived as an alternative to compliance with legal obligations or as an excuse to avoid administrative sanctions. The right to the protection of personal data is a fundamental right in Europe and its effective protection should not depend solely on the willingness of a company. Strong enforcement and dissuasive sanctions are required when companies fail to comply with the law.

Article 23- Data protection by design and by default

BEUC welcomes the introduction of the principles of data protection by design and by default in the draft Regulation, making it compulsory for data controllers to implement appropriate measures to comply with them. The two principles will help to

empower data subject's control and enhance the enforcement of the data protection legislation.

Article 23.1 establishes the principle of **data protection by design**, which would require privacy and data protection are embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal. BEUC welcomes flexibility provided to data controller to comply with the general principles. BEUC would also welcome the inclusion of a reference to the use of Privacy Enhancing Technologies (PETs) as a tool to implement technical solutions to comply with the principle of data protection by design.

As regards the principle of **data protection by default,** BEUC believes that Article 23.2 should be revised to make it explicit that the privacy settings on services and products should by default comply with the general principles of data protection, such as data minimization and purpose limitation.. The data subject should have the choice to change the privacy settings and decide whether he wants to share his personal data and with whom. Privacy settings are an important aspect of online privacy. Consumers expect companies to create privacy settings that provide transparency and control over the ways that organizations collect, use, and store personal information.

BEUC is also concerned that Article 23 only addresses the data controller. However, the processor should also be obliged to implement privacy by design and privacy by default while processing personal data on behalf of the controller. Such a requirement should be added in Article 26 which defines the obligations for data processors.

Article 24-Joint controllers

BEUC welcomes the provision on joint controllers (Article 24) and the introduction of an obligation to define their respective responsibilities for compliance with the obligations by means of an arrangement between them, while failure to comply with this obligation will entail administrative sanctions according to Article 79.5.e. In practice, the chain of responsibility and liability is getting difficult to follow for data subjects not only as regards data controllers but also controllers and processors (e.g. cloud computing), let alone that the distinction between data controller(s), data processor(s) and third parties is blurred. Although Article 26 requires the controller to define the respective responsibilities with data processor processing data on his/her behalf, BEUC would recommend including a specific provision on joint responsibility between the controller and the processor, allowing the data subject to seek redress from each of them.

Article 25- representatives of controllers not established in the Union

BEUC regrets the exception from the requirement to designate a representative in the European Union for data controllers not established in the EU (Article 25). The representative is expected to be the contact point for both data protection authorities and the data subject and therefore any exception must be fully justified or otherwise deleted.

Article 28- Documentation

Article 28 introduces the obligation for controllers and processors to maintain documentation of the processing operations instead of the cumbersome requirement for notification of the data controllers' personal data handling practices, which exist in the current framework. Under the new Framework, data controllers should document any processing operation and be able to demonstrate compliance upon request to the Data Protection Authorities.

The documentation obligation, as defined in Article 28.2, includes the most relevant information and should not be simplified. The contact details of the controller and of the data protection officers, the types of personal data, the recipients of personal data, the purposes for processing, possible transfers to third countries and retention periods are the minimum information that any responsible and accountable organization needs to keep record of. It will also make the checking by Data Protection Authorities easier and will help to improve monitoring of compliance and enforcement.

However, in order to comply with their obligations under Article 22, data controllers will in any case be able to demonstrate compliance with the legislation and the effectiveness of the undertaken measures. We would therefore support the proposal put forward by the European Data Protection Supervisor[5], to introduce an obligation to keep an inventory of all processing operations that would encompass general information, namely the contact details of the controllers (and joint controllers and processors if applicable), the contact details of the data protection officer and the description of the mechanisms implemented to ensure the verification of the measures undertaken in order to ensure compliance. The more specific information should be part of an additional obligation to inform data protection authorities upon request.

As regards the exception from the documentation obligation for organizations with less than 250 employees, BEUC would suggest its deletion or its replacement with a criterion based on the nature of the processing activities, the number of personal data involved and the number of data subjects the enterprise processes data about. The exception should only apply to those enitities that are processing data as an accessory activity.

Article 31- Notification of a personal data breach to the supervisory authority

Article 32- Communication of a personal data breach to the data subject

BEUC welcomes the introduction of a horizontal data breach notification obligation for the controller, beyond the telecommunications sector. Consumers may suffer at least the same harm from the undue disclosure of their bank account details as from the disclosure of their telephone bills.

Individuals have the right to be informed about the use of their personal data, including when their data have been compromised. According to the research carried

[5] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012.

out by the UK consumer organisation Which?, the vast majority of UK consumers (74%) would always wish to be notified of a data breach.

The draft Regulation introduces a dual system of notification, according to which all breaches must be notified to the Data Protection Authorities (Article 31), while only those breaches that adversely affect the protection of personal data and privacy should be notified to the individuals (Article 32).

However, the definition of what constitutes a breach adversely affecting is only partly provided in Recital 67. In order to ensure a consistent approach across Europe and legal certainty, BEUC would suggest including the definition in Article 32. Such a definition should be broad and encompass not only those breaches that result in economic loss, but also breaches which may cause immaterial damages, such as any moral and reputational damages. Additional criteria, such as time spent in attempts to rectify the breach and distress should also be considered when assessing the adverse effect.

BEUC supports a risk-based definition of the adverse effect of data breaches. In order to determine the level of risk, both quantitative and qualitative indicators need to be considered. For example, the type of data, the number of individuals affected and the amount of data breached would have to be considered.

As regards the content of the notification, the requirements set in article 32.2 should also comprise a description of the consequences of the personal data breach (article 31.3 d)); in addition ,the individual should also be informed about his/her rights and be provided with the contact details of the Data Protection Authority and of consumer associations that could help him seek redress.

BEUC would also suggest including a specific requirement for the notification to be clear and comprehensive, i.e. without technical jargon. It should be sufficient for the individual to read the notice to understand the risks and the recommended actions.

BEUC agrees that only those breaches that adversely affect the individual should be notified to data subjects. A general obligation to notify individuals whenever personal data has been compromised might be counter-productive and lead to "notification fatigue" and desensitization.

BEUC regrets the fact that only the data controller is required to notify breaches. This obligation should also cover breaches occurring while personal data is being processed by the data processor. In this case, the data controller should bear the responsibility to notify.

As regards the notification to the data protection authorities, BEUC believes that the notification to take place as soon as possible and without due delay, and not beyond 72 hours after the controller becomes aware of the data breach.

We would also suggest that a specific deadline is introduced for the DPA to act on a breach notification, as well as a deadline within which the data controller should notify the breach to the data subject.

Articles 33-34 – Data Protection Impact Assessment and prior authorization

BEUC welcomes the introduction in the EU Data Protection framework of an obligation for the controller and the processor to carry out an assessment of the impact on the protection of personal data of the processing operations that present specific risks. The implementation of meaningful PIAs that require compliance with privacy standards figures in the Madrid Privacy Declaration that was adopted by the International Conference of Privacy and Data Protection Commissioners in November 2009.

A robust framework of Privacy Impact Assessment can be an effective tool to address the challenges of a fast evolving ICT sector and help identify the risks to consumers' fundamental rights to privacy and to protection of personal data at an early stage. As such, PIA is an integral part of the privacy by design principle. It also enables data controllers and processors to demonstrate compliance with the requirements of the Regulation.

A DPIA should also be carried out when it is not clear whether a processing activity poses serious risks in order to allow for a thorough assessment of the associated risks.

We are also concerned with the limitation of processing operations to processing on a large scale when information about the sex life, health, race and ethnic origin or for the provision of health care etc (Article 33.2.b). This type of information is sensitive personal data and therefore a PIA should be mandatory irrespective of the scale of processing.

BEUC would also suggest introducing in Article 30 a specific requirement for the DPIA or at least of a summary to be made publicly available. It should be for the national Data Protection Authorities to maintain a registry of PIAs, similar to the system in the District of Columbia in Canada[6]. This would allow individuals to consult the PIAs and increase their confidence in the handling of their personal data. It goes without saying that the PIAs or their summaries should be published in a reader-friendly format.

BEUC would support the audit of any PIA by the Data Protection Authorities to ensure that it fulfills the conditions set in the Regulation. This would increase the reliability of PIAs and would also facilitate the establishment of a central registry open to consultation by all stakeholders.

Moreover, the obligation to carry out an impact assessment needs to be based on the precautionary principle; article 33.1 should be reworded stating that the impact assessment should be carried out when processing operations "are likely" to present specific risks to the rights an d freedoms of data subjects[7]

Articles 35-37- Data Protection Officer

BEUC welcomes the introduction of the obligation for both controller and processor to appoint a Data Protection Officer (DPO) within the framework of the accountability

[6] PIAF, Privacy Impact Assessment Framework for data protection and privacy rights, Deliverable 1 http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf

[7] This will also align the wording of article 33.1 with the wording in articles 34.2 a) and 33.6.

principle. DPOs are familiar with the problems and the processing activities of the entity they work for and can therefore provide valuable advice as to implementation of the Regulation and monitor compliance. It is also expected that the appointment of DPO will help to in crease awareness of data protection rules within the entity; according to Eurobarometer (2008) survey, only 13% of people responsible for data protection within companies said that they were very familiar with the provisions of data protection law[8].

The appointment of DPO should be mandatory. As regards the proposed threshold of 250 employees for requiring the designation in an enterprise, this is not justified, given that all Small and Medium Enterprises would escape this obligation. BEUC considers that the determining factor should not be the number of employees, but the nature of the processing activities, the number of personal data involved and the number of data subjects the enterprise processes data about. The exception should only apply to those enitities that are processing data as an accessory activity.

DPOs must have expert knowledge of data protection law and sufficient experience to carry out the assigned tasks. Given their special role, there needs to be a mechanisms in place to check and verify the qualitification of DPAs. This will also be to the benefit of data controllers, who risk administrative sanctions for failing to appoint DPO or for not respecting the conditions for its appointment, according to article 79.6.j. DPAs could also organize regular training seminars for appointed DPOs.

The draft Regulation requires DPOs to be independent from the data controller or processor. However, in practice there will most often be an employment relationship between the two parties. BEUC would therefore suggest further strengthening the independence of DPOs by requiring the controller or processor to submit a fully justified report to DPA in case of dismissal of DPO (article 35.7). In addition, in case of disagreement between the DPO and the controller or processor, and in case of doubt as to compliance with rules, it should be for the supervisory DPA to provide guidance.

Articles 38-39– Codes of conduct and certification

BEUC is concerned with the encouragement of the codes of conduct to be developed by controllers and processors. Self regulatory codes can only be endorsed if they entail an added value for consumers' rights by offering a higher level of protection, are backed up by suitably robust auditing or testing procedures and provide for independent complaint handling and enforcement mechanisms.

However, Article 38 does not address these concerns. On the contrary, it only provides for the possibility for industry associations to submit the draft codes to supervisory authorities, which can only issue a non-binding opinion. Furthermore, the draft Regulation is rather weak when it comes to complaint handling mechanisms the development of which is left exclusively to data controllers and processors. Similar inter-company complaint handling schemes should by no means by recognized as out of courts dispute resolution procedures given that they lack independence.

[8] Eurobarometer survey on data protection in the EU, February 2008.

The development of EU certification schemes and privacy seals could become effective means to ensure 'privacy compliant' or even 'privacy enhancing' IT products, websites, companies and services. It will also provide an incentive for developers and providers of such products and services to invest in better privacy protection, while allowing users to make an informed and quicker choice.

BEUC supports the establishment of EU certification schemes, including European Privacy Seals, as long as clear certification criteria are developed and the administration is entrusted to independent third party organisations. The establishment of a Certification Authority for the issuing of the seals and the accreditation of specially trained and tested independent experts, who carry out the primary evaluation of the products provide for additional safeguards.

It is therefore regrettable that the Commission has reserved the right to specify the criteria and requirements, including the conditions for granting and withdrawal through delegated acts. It would be preferable if more substantive rules are included in Article 39 to ensure legal certainty.

CHAPTER V – Transfer of personal data to third countries or international organizations (Articles 40-45)

As more and more processing operations take place in a global context, it is important to adapt the EU framework with the aim of ensuring the free flow of data, while guaranteeing the level of protection for data subjects' rights. The draft Regulation recognizes the new reality and abandons the presumption that personal data may not be transferred without an adequacy level of protection, setting instead a number of principles that must be fulfilled when personal data are transferred outside the EU.

BEUC welcomes the inclusion among the factors to be considered when assessing the **adequacy** of level of protection elements related to rule of law, the existence of effective and enforceable rights and means of redress for data subjects (Article 41.2.a).It is also positive that the adequacy recognition will also depend on the international commitments of the third country, which would also include the ratification of the Council of Europe Convention.

In the absence of an adequacy decision, the draft Regulation allows for the transfer of data provided that the controller and/or the processor has adduced appropriate safeguards in a legally binding instrument. Such safeguards will be provided by Binding Corporate Rules (BCRs), standard data protection clauses approved by the Commission or adopted by a DPA.

BEUC regrets that the proposal opens the possibility for transfer when safeguards are not provided in a legally binding instrument (Article 42.5), which might urge controllers to adopt codes of conduct. A similar derogation cannot be justified and therefore it should either be deleted or limited to few specific cases.

It should also be clarified that that transfers should not be possible for those countries for which the European Commission has already adopted a decision not recognizing the adequate status, such as Bahamas and South Africa

Binding Corporate Rules have already been endorsed by Article 29 Data Protection Working Party and therefore their explicit recognition as an adequate mechanism for transfer of data to third countries in Article 43 is welcome. It is important that BCRs are binding and enforceable upon all members of the controller's and processor's undertaking and that implementation will require the approval by the supervisory authority.

BEUC is concerned with the broad scope of Article 44 on **derogations**. It should be made explicit that derogations can only apply for a restricted number of cases of occasional transfer that cannot be qualified as frequent, massive or structural, as pointed out by Article 29 Data Protection Working Party[9] and the European Data Protection Supervisor.

Furthermore, the consent of the data subject can be used as derogation to the rules on international transfers. As already outlined, it is questionable whether the data subject has the sufficient knowledge to fully assess the implications of transfer of his/her personal data to a third country without an adequate level of protection and with no safeguards from the controller. Article 44.1 should therefore be deleted.

We are also concerned with the broad definition of the "public interest" which would also cover the transfer of personal data to third countries for the prevention, investigation, detection and prosecution of criminal offences (Recital 87). A similar provision would increase the risk of abusive transfers to law enforcement authorities without any safeguard for the protection of data subjects' fundamental rights.

As regards **international cooperation** for the protection of personal data, Article 45 aims at enhance cooperation between data protection authorities in **enforcing the law.** Although such cooperation is crucial, we are concerned with the role envisaged for stakeholders in enforcing the law. Such a provision relates to the recently announced Consumer Privacy Bill of Rights by the US President which foresees the development of codes of conduct as a tool to enforce the law. BEUC is concerned that such schemes of self- and co-regulation fail to provide a robust enforcement system.

Lastly, BEUC regrets the deletion during the inter-service consultation of a provision that would have prohibited the transfer of personal data based on **orders or requests from non-EU courts, tribunals, administrative authorities and other governmental entities**. It stated that in cases where a third country requests the disclosure of personal data, the controller or processor had to obtain prior authorisation for the transfer from its local supervisory authority. This provision is particularly relevant with regards to requirements under US law for the disclosure of data, in particular based on law enforcement requirements or e-discovery requests. The US uses instruments such as the Foreign Intelligence Surveillance Act (FISA) and the Patriot Act to retrieve data on (e.g.) the political activities of foreign individuals, who may have no links whatsoever with the USA, via companies with US offices. We would suggest that this article is added in a separate new article.

---

[9] Working Document of Article 29 Working Party of 26 November 2005 on a common interpretation of Article 26.1 of Directive 95/46 of 24 October 1995 (WP114).

CHAPTER VI – Independent Supervisory Authorities (Articles 46-54)

BEUC welcomes the provisions of the draft Regulation that establish explicitly the **independent** status of Data Protection Authorities in order to ensure the effectiveness and reliability of the supervision of compliance with the legal framework.

However, we regret the absence of specific standards for the **funding** of the operations of Data Protection Authorities. Article 47.5 only calls upon Member States to ensure that DPAs are provided with adequate human, technical and financial resources[10]. Adequate funding is a key element to ensure the independence of DPAs. Such funding should be proportionate to the number of data controllers DPAs regulate and the individuals whose personal data is processed.

We would therefore suggest that specific provisions are added in Article 47 that would outline complementary sources of funding for DPAs. In its document 'the future of privacy" Article 29 Data Protection Working Party has suggested alternative sources of **funding**, which may range from a fully fee-based model (based e.g. on notification fees and the levying of fines for breaches of the law) to a fully State-funded model[11]. We would also like to underline that in many cases, DPAs may be reluctant to impose sanctions against companies due to the increased costs of counter-litigation if companies challenge to justice the sanctions imposed. This may undermine the capacity of DPAs to undertake action.

As regards the provisions on the competence of DPAs, BEUC is concerned with the notion of a **lead authority to be determined by the main establishment** of the data controller or processor. Article 51 aims to establish the competent authority for organizations operating in more than one Member State. Article 4.13 defines the "main establishment" of data controller as the place where the main decisions as to the purposes, conditions and means of processing are taken. However, this definition is not appropriate for undertakings with decentralized decision making structure, where the central administration and the place where management decision about data processing are made differ. It would be more appropriate to introduce a number of specific factors/criteria that would need to be considered to assess the lead authority, such as the number of data subjects whose personal data is affected.

It should also be made explicit that the powers of the lead authority are not exclusive and that cooperation between all relevant DPAs is ensured. Otherwise, there is significant risk that data controller will decide to get established in those Member States with the less stringent rules, given that a degree of flexibility would still be left to Member States thus increasing the risk of forum shopping.

Furthermore, the rules on the lead authority will only apply where the controller has an establishment in the European Union. **Article 51 does not cover those cases where there is no establishment in the** EU, in cases where the processing

[10] See also Article 29 Data Protection Working Party letter to Vice-President Reding http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120404_letter_to_vp_reding_resources_en.pdf

[11] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf.

activities are related to the offering of goods and services to data subjects residing in the Union or the monitoring of their behavior. Given that similar processing activities may easily affect data subjects in multiple EU Member States, specific rules on the assignment of a lead authority should also be defined. BEUC considers that lead authority should be the authority of the Member State where most data subjects have been affected, or the Member State where a specific complaint has been lodged.

A key issue which is not addressed in the draft proposal is who should be responsible for the appointment of the lead authority (the authority or the controller) and how disputes regarding appointment of the lead authority are to be solved.

Article 52 provides for the duties of supervisory authorities, including the power to hear **complaints lodged by data subjects** (52.1.b). Given that the lead authority might be different from the one of the residence of the data subject, a number of practical problems need to be solved, including who bears the costs for translation and/or interpretation. These should not be borne by the data subject, as it would be major obstacle to the exercise of his fundamental right to redress.

CHAPTER VII – Cooperation and Consistency (Articles 55-72)

BEUC welcomes the focus of the draft Regulation on enhancing **cooperation** between Data Protection Authorities. Article 56 empowers DPAs to undertake joint operations, including joint investigations and joint enforcement measures. Article 55.2 introduces the duty to take action upon request of another DPA within one month. Failing to comply with this duty, the DPAs may take provisional enforcement or compliance actions in the other Member State. Nevertheless, we are concerned about the nature and the scope of similar measures since it might raise problems of interference with national procedural and constitutional law.

Strengthening the cooperation between DPAs is crucial, given that a data breach may well affect data subjects across Europe and beyond. However, this should not be the only mechanisms for ensuring cross-border enforcement of data protection laws. To this, the experience with the Consumer Protection Cooperation Regulation needs to be assessed. A number of interesting conclusions can be derived from the most recent report on the implementation of the CPC Regulation published in March 2012. Despite the fact that the CPC network has already been established for several years (since 2006), there is still no uniform understanding among the national authorities about how to use the cooperation tools. Furthermore, the average time for the handling of mutual assistance requests is 92 days. Article 55.2 of the draft Regulation requests DPAs to act within 30 days[12].

With regards the "**consistency**" mechanism, BEUC sees the merits of the need for a more coherent approach of DPAs to issues of common interest. However, we are concerned that almost every case when a DPA considers the adoption of measures against a company operating internationally will trigger the consistency mechanism. There needs to be a threshold in the draft Regulation to ensure that consistency only applies to processing that raises serious risks to data subjects across Europe.

[12] http://ec.europa.eu/consumers/enforcement/docs/comm_biennial_report_2011_en.pdf

Furthermore, the draft Regulation allows the European Commission to intervene extensively in the context of the consistency mechanism. In particular, the Commission can ask for the consistency mechanisms to be applied, but can also suspend a measure adopted by a DPA if there are serious doubts as its effectiveness (Article 60). BEUC agrees with the European Data Protection Supervisor to limit the any suspension to a clear breach of EU law subject to scrutiny of the Court of Justice[13]. The same concerns are raised by the power of the European Commission to overrule a decision of a national DPA through an implementing act (Article 50.1 and 62.1.a).

The provisions of the draft Regulation may undermine the independence of DPAs and subject their decisions to the external influence of the European Commission. The Commission could adopt its own Opinion but without any effect on the decision of the European Data Protection Board, while in cases of serious conflict it should be for the European Court of Justice to decide.

Lastly, BEUC welcomes the provisions on the establishment of the **European Data Protection Board** to replace the Article 29 Data Protection working party, particularly with regards to its independence. The status and the legal nature of the Opinions of the Board is necessary to ensure that they become binding particularly when they concern the interpretation of provisions of the Regulation.

CHAPTER VIII – Remedies, Liabilities and Sanctions (Articles 73-79)

Efficient redress is a key component of a data subject's empowerment. Although the current Directive already foresees the possibility for individuals to seek redress and compensation for damages suffered as a result of a data breach, in practice this provision has not been implemented effectively. The high costs related to individual litigation, as well as the legal uncertainty as regards competent forum and applicable law act as a deterrent in the enforcement of data subject's rights and an impediment to the fundamental right of access to justice.

BEUC welcomes the introduction of provisions that provide for **several redress mechanisms** with the view to facilitate enforcement by the data subject (Article 73). It is important that individuals can lodge a **complaint with any DPA**, namely the one of their place of residence. However, it must be clarified that any costs related to translation and transfer of complaint to the competent DPA of another Member State should not be born by the data subject.

As regards the right to **judicial remedy** against the controller and the processor, BEUC welcomes the provision enabling the individual to lodge the complaint either before the court of the country of establishment of the controller or the court of the residence of the data subject. Although this rule might lead to several courts being seized in different Member States, particularly in cross border cases, the complexity can be solved through the establishment of clear rules regarding the competence of courts. For instance, it can be clarified that the court of the place of the most affected data subjects is the competent one and the others should suspend

[13] Opinion of the European Data Protection Supervisor on the data protection package reform, 7 March 2012.

proceedings until the ruling is issued. It should however be ensured that the ruling can be recognized and executed in all other Member States.

Despite our support for the proposed redress mechanisms, we believe that additional more cost and time efficient routes for consumers to enforce their rights should be considered.

BEUC welcomes the right for organizations **or associations defending data subject's rights** to lodge a complaint before a supervisory authority (Article 73) or to bring an action to court (Article 76) on behalf of data subjects. However, we regret that the proposal has stopped short of introducing fully fledged collective **judicial actions** whereby representative bodies can claim compensation for the damages suffered by data subjects.

BEUC supports a system of judicial collective action on the basis of Europe's legal tradition and the experiences from EU Member States. A number of safeguards need to be included to ensure that the system is not abused. BEUC has developed ten golden rules for a European judicial collective action[14].

BEUC therefore calls for a specific provision to be included in Article 77 which allow representative organization to bring judicial actions for compensation. There should be a clarification as regards the **quantification of damages and the calculation of compensation**. To this end, the possibility for **flat rate compensation** to be provided in case of data breaches should be considered. When it comes to data breaches, the damages suffered are typically too small on an individual scale and would entail significant and disproportionate costs; however, the collective damage is significantly more substantial. An illegal behavior of abuse of personal data can easily affect a high number of people, especially in the online environment, where online services are cross-border and often provided from outside the EU. Furthermore, damages suffered are often intangible and it is difficult to assign a value and determine the responsibility of the involved parties, while in some cases, there might be no immediate damages, such as when confidential data (credit card numbers) are leaked.

It should also be clarified that consumer organizations are entitled to bring actions for breaches of data protection law. In some EU Member States, consumer organizations can only act for breaches of consumer protection legislation, and data protection falls outside their remit. Nevertheless, consumer associations are credible entities with long experience in defending consumers and should therefore be entitled to act in the field of data protection. It should also be clarified that **damages** should include not material and quantifiable damages, but also immaterial damages and distress.

BEUC also welcomes the **joint liability** of data controller and data processor when it comes to liability. It might be difficult for the data subject to determine which entity is the data controller who bears the liability in cases of damages suffered.

Article 79 aims to strengthen the mechanisms for **sanctions** in case of data protection infringements. The sanctions foreseen resemble the ones established

[14] European Group Action, BEUC's ten golden rules
http://docshare.beuc.org/docs/2/MMOLGAFDFOMBPINPIJPPOEMDPDBW9DB67K9DW3571KM/BEUC/docs/DLS/2008-00394-01-E.pdf

under competition law and aim to act as a major deterrent for companies involved processing of personal data. However, BEUC considers that the fines imposed on companies could also be used to finance the actions of organizations defending the rights of data subjects. Furthermore, safeguards need to be included if fines are to be used mainly for the funding of DPAs to ensure that the system is not abused.

As regards the **exceptions** foreseen for processing by natural persons without commercial benefit and for entities below 250 employees for which personal data processing is an activity ancillary to its main activities, BEUC considers that the important factor should not be on the number of employees but rather on the nature of the activities. For example, consumer organizations may well carry out surveys with the aim of advising consumers that might involved the processing of personal data. Such an activity is ancillary to the normal activities of consumer organizations and should therefore be exempted from the scope of Article 79.

CHAPTER IX – Provisions relating to specific data processing situations (Articles 80-85)

Chapter IX leaves room for specific national rules for specific processing situations related to freedom of expression, health, employment, professional secrecy and churches and religious associations.

Article 80: Processing of personal data and freedom of expression

BEUC welcomes the exemption from the regulation when personal data is carried out for journalistic purposes or for the purpose of artistic and literacy expression. The freedom of expression must be balanced with the right to protection of personal data to ensure the effective exercise of both. To this end, an assessment on a case by case basis may be required to ensure that the right to data protection is not misused to hinder freedom of expression and freedom of information.

We would also suggest that the notion of journalistic purposes is clarified to include not only the traditional media, but also new all activities whose object is the disclosure to the public of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper or radio waves or an electronic medium such as the internet) and of the nature (profit-making or not) of those activities, in line with the ruling of the European Court of Justice[15].

Article 81- Processing of personal data concerning health

Article 81 foresees a number of exceptions to the general prohibition of processing sensitive health data: we support those exceptions as they ensure a good balance between the right to privacy, consumer safety and public health interests but we think that certain aspects should be further clarified to prevent abuses. Moreover we would like to stress that the use of sensitive health data for marketing purposes

[15] C-73/07- Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy.

should remain prohibited. Tracking and profiling technologies in health related web sites should not be allowed.

Article 81 allows the use of compiled health data for research purposes, for better managing the health care expenditures, for monitoring and improving the quality, the safety and the effectiveness of medicines, medical devices. Whilst we do not question the benefit of this for the safety of the individuals and for public health, we question the actual possibility of ensuring the anonymity of data. Technological advances in data analysis and the combination with other data set could endanger anonymity and lead to the identification of individuals. Unanswered questions remain also as to who exactly would have access to such data. For example, would the research sector include pharmaceutical companies? Would public accessibility mean that insurers can access the data? The legislation also lacks an indication as to how the amount of information seen will differ according to the role of the person accessing it. For example, how will the data patients see differ from the data that is available to care staff, policy makers, and third party researchers?

It is crucial that only authorised and specifically trained health care professionals have access to patients' health records. Art.81 mentions that the processing of data could be done by a person other than the healthcare professional provided that he/she is subject to an equivalent obligation of confidentiality. The definition of another person should be further specified to prevent abuses and inconsistency with the other provisions of the legislation.

Article 82- Processing in the employment context

BEUC does not see the need for the special treatment of processing in the employment context. When personal data in the employment context is processed, the general provisions of the Regulation will apply. If the exception for national rules is maintained, it should be clarified that such rules should be compatible with the general provisions and that they simply aim to complement or particularize the Regulation to the national context.

Article 83- processing for historical, statistical and scientific research purposes

BEUC welcomes the exemption when personal data is processed for historical, statistical and scientific purposes. It should however, be stressed that the preferred option should be the processing of anonymised data and that only when it is impossible for the specific research, personal data should be processed when the conditions of Article 83 are met.

CHAPTER X – Delegated acts and implementing acts (Articles 86-87)

The draft Regulation often empowers the European Commission to adopt delegated and implementing acts. Although such acts can in certain cases ensure a uniform implementation of the Regulation, BEUC is concerned that the extensive use of this mechanism, as foreseen by the proposal, will undermine the objective of establishing a clear and comprehensive set of rules to the detriment of both data subjects and businesses. We are also concerned about the time required for all delegated acts to

be issued; according to the estimated financial impact statement accompanying the Regulation proposal, only two delegated acts will be administered per year, and therefore a period of ten years will be required to adopt all acts and achieve legal certainty.

BEUC would suggest that the number of provisions subject to the adoption of delegated and implementing acts should be significantly reduced and limited to those provisions addressing non-essential issues, such as design requirements, criteria for technical measures etc. Furthermore, the mechanism of Article 86 could be used as the basis to adopt sector-specific rules clarifying the application of the general framework to specific areas of law. We would therefore suggest the possibility for the adoption of delegated acts and implemented acts is **maintained** only for the following provisions:

- Article 8.3 referring to the definition of criteria and requirements to verify parental consent in case of processing of personal data of a child below the age of 13 years old;
- Article 14.7 with regards to the modalities for the provision of information to the data subject;
- Article 15.3 on the content of the communication to the data subject of the personal data undergoing processing following a request to access data;
- Article 22.4 on the appropriate measures to be adopted by the data controller to ensure compliance in accordance with the principle of accountability which requires a certain degree of flexibility;
- Article 23.3 on the design requirements for the application principle of data protection by design on specific products and sectors;
- Article 26.5 regarding the measures to be adopted by the data processor in order to comply with the obligations established in the Regulation;
- Article 28.5 on definition of criteria and requirements for the documentation obligation;
- Article 30.3 which deals with technical aspects of security;
- Article 35.11 on the qualification of the data protection officer;
- Article 37.2 regarding the tasks, certification, status, powers and resources of the data protection officer;
- Article 43.3 on further specifying the criteria and requirements of binding corporate rules;
- Article 79.6 on the update of the amounts of the administrative fines

As regards the rest of the cases, it is crucial that further clarification is included in the current Regulation, since they refer to substantive and essential elements and therefore call for legal certainty. This is the case of the following provisions:

- Article 6.5 which foresees the adoption of sector-specific rules clarifying the application of the legitimate interests of the data controller as a ground for lawful processing; there is the riska that unless clearly specified, the legitimate interests of the controller may be invoked by controller as the legal ground for processing circumventing even when there is no appropriate legal ground;
- Article 9.3 referring to sensitive data; the processing of sensitive data requires an additional layer of protection due to the nature of the information they can reveal about an individual and therefore the conditions and the safeguards for their processing must be clearly defined in the draft Regulation.

Alternatively, this could be the object of opinions/reports of the European Data Protection Board;

- Article 12.4 regarding the definition of threshold above which requests to access and correct one's own data will be considered excessive. Otherwise, there is a risk that Member States use different thresholds thus hindering the effective exercise of the individual's rights;
- Article 17.9 on the implementation of the right to be forgotten. Given the interaction with fundamental freedoms, the conditions for deleting links, copies from publicly available communication services should be defined upfront;
- Article 18 regarding the right to data portability, the effective implementation of which requires the development of interoperable or compatible standards;
- Article 20.5 reserving the right for the Commission to define the safeguards for the data subject when profiling is allowed. This provision touches upon essential and substantive elements of data subject's protection;
- Article 31.5 which refers to the threshold for data breach notification; unless a threshold is clearly defined in the Regulation, all breaches might have to be notified to the data protection authority;
- Article 32.5 on the communication of data breach to the data subject. It is crucial to define when a breach will seriously affect the rights of the individual and will therefore require notification;
- Article 33.6 regarding the definition of operations presenting specific risks and therefore subject to a data protection impact assessment;
- Article 34.8 on the definition of the high degree of specific risk demonstrated by an impact assessment;
- Article 39.2 on certification mechanisms and privacy seals. For certification and seals to be endorsed by data subjects, full compliance with the legal framework and high standards of protection need to be ensured. It is therefore important that the conditions for the granting and the recognition within the EU are clearly defined;
- Article 44.7 on the notion of the public interest that might justify a derogation from the rules on transfer to third countries;
- Article 81.3 on the notion of public interest in relation with the processing of personal data concerning health;
- Article 83.3 regarding the criteria for limiting data subject's rights for the processing of historical, statistical and scientific research purposes.

END

DANSKE REVISORER FSR

Justitsministeriet
EU-formandskabssekretariatet
Slotsholmsgade 10
1216 København K

Att.: Johan K. Legarth

28. juni 2012

Pr. e-mail : jm@jm.dk

FSR – danske revisorer
Kronprinsessegade 8
DK - 1306 København K

Telefon +45 3393 9191
fsr@fsr.dk
www.fsr.dk

CVR. 55 09 72 16
Danske Bank
Reg. 9541
Konto nr. 2500102295

Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) – j.nr. 2012-3756-0005

Tak for muligheden for at kommentere forslaget.

Vi har ingen bemærkninger.

Med venlig hilsen

Jakob Dedenroth Bernhoft
juridisk chef

Fra: Kirsten Fly Malling [kfm@sdu.dk]
Sendt: 28. juni 2012 15:45
Til: Justitsministeriet
Cc: Jens Oddershede; Bjarne Graabech Sørensen; Jacob Schmidt; Merete Ruager; Karin Bruun; Jørgen Schou; journal mailbox
Emne: Høring over Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i.f.m. behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

Justitsministeriet
EU-formandskabssekretariatet
Slotsholmsgade 10
1216 København K

Justitsministeriets j.nr. 2012-3756-0005.
Syddansk Universitets j.nr. 077-2012.

Justitsministeriet har ved e-mail af 11. maj 2012 anmodet universitetet om evt. bemærkninger til ovennævnte høring.

Syddansk Universitet har ingen bemærkninger.

På rektors vegne

Jørgen Schou
Kontorchef, Juridisk Kontor, Ledelsessekretariatet

Tlf. 6550 1040
Mobil 6011 1040
Fax 6550 1090
Email js@sdu.dk
Web http://www.sdu.dk/ansat/js
Adr. Campusvej 55, 5230 Odense M

Justitsministeriet
Slotsholmsgade 10
1216 København K

jm@jm.dk

Landbrug & Fødevarer

Axelborg, Axeltorv 3
DK 1609 København V

T +45 3339 4000
F +45 3339 4141
E info@lf.dk
W www.lf.dk

CVR DK 25 52 95 29

Høring over forslag til databeskyttelsesforordning, j.nr. 2012-3756-0005

Justitsministeriet har den 11. maj 2012 fremsendt forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordning). Landbrug & Fødevarer takker for muligheden for at bidrage med et høringssvar.

Generelle bemærkninger

Landbrug & Fødevarer mener, at det er vigtigt at forhindre personlige oplysninger fra at blive offentliggjort på en måde, der krænker retssikkerhedsmæssige hensyn. Det er samtidig afgørende at sikre fleksibilitet og undgå unødig administrative byrder for erhvervslivet. Landbrug & Fødevarer ser generelt denne forordning som en god mulighed for at samtænke disse to hensyn. Det bør være forordningens mål at fremme beskyttelsen og samtidig opdatere reglerne på persondata-området, således at de kan følge med de teknologiske fremskridt.

Landbrug & Fødevarer finder det som udgangspunkt hensigtsmæssigt, at adgangen til at dele oplysninger imellem offentlige myndigheder er ubesværet, fx for at lette virksomheder og privat personer for unødvendige administrative byrder ved at indsende de samme oplysninger til flere myndigheder. Det offentliges udveksling af oplysninger forudsætter dog, at der er et helt grundlæggende udgangspunkt, der sætter borgeres og virksomheders retssikkerhed i fokus, og at der ikke gives køb på retssikkerheden som grundlæggende princip.

Landbrug & Fødevarer mener imidlertid, at forordningen, i den foreliggende form, indeholder en række bestemmelser, der trods den gode intention indebærer uhensigtsmæssige administrative byrder, jf. de uddybende bemærkninger til de enkelte bestemmelser nedenfor.

Endvidere skal det pointeres, at det foreslåede og ufleksible bødeniveau forekommer helt ude af proportioner, og at adgang til administrative bøder i denne størrelsesorden på dette område er stærkt betænkeligt.

Landbrug & Fødevarer bifalder forordningens formål med at gøre lovgivning på persondata-området i EU ensartet. Det vil væsentligt øge gennemsigtigheden på området, særligt for internationale virksomheder. Landbrug & Fødevarer finder dog, at forordningen i sin nuværende udformning overlader meget til senere udmøntning af Kommissionen, hvilket kan risikere at medføre en usikker retsstilling, særligt i den kommende forordnings første år, men også på længere sigt. Virksomheder risikerer, at fastsatte arbejdsgange underkendes, uden at der har været mulighed for at gøre sig bekendt med risikoen herfor, fordi det fulde lovkompleks ikke er på plads. Landbrug & Fødevarer opfordrer til, at der skabes helt klare retningslinjer, så aktørerne fra starten kan danne sig et overblik over reguleringen.

Bemærkninger til de enkelte bestemmelser:

Art. 6

Landbrug & Fødevarer mener, at kravet om eksplicit samtykke medvirker til at sikre, at den registrerede har kontrol over hvilke oplysninger, der registreres, og hvad formålet med disse registreringer er. Landbrug & Fødevarer bemærker dog at det skal sikres, at kravet ikke pålægger virksomheder unødvendige byrder og infleksibilitet. Landbrug & Fødevarer anser det som vigtigt, at der er adgang til simpel sikring af det udtrykkelige samtykke.

Art. 17

Landbrug & Fødevarer finder, at "adgangen til at blive glemt og ret til at blive slettet" udgør et vigtigt skridt for at sikre, at private selv har kontrol over deres oplysninger, og bifalder denne bestemmelse. Landbrug & Fødevarer finder det fornuftigt, at bestemmelsen er begrænset, således at oplysninger kun kan bedes slettet eller glemt, såfremt de ikke længere er nødvendige for det formål, som de er blevet indsamlet til. Såfremt denne undtagelse ikke fandtes, kunne man havne i nogle meget uhensigtsmæssige situationer, hvor der savnes information til et konkret projekt.

Art. 18

Landbrug & Fødevarer er bekymret for, at den registreredes ret til at få udleveret en kopi af registrerede oplysninger kan blive byrdefuldt for virksomheder. Der bør tages højde for dette i den endelige forordning.

Art. 28

Landbrug & Fødevarer mener, at kravet om at opbevare dokumentation for enhver behandling af registrerede personoplysninger er meget omfattende og virker unødigt byrdefuldt. Denne dokumentation vil ved større virksomheder hurtigt blive utrolig omfattende, uden at der ses egentlig gevinst ved dokumentationen. Kravet bør begrænses, således at der ikke er krav om, at enhver behandling dokumenteres, men blot behandlinger, der er af større betydning.

Art. 31

Landbrug & Fødevarer mener, at kravet om, at brud på persondatasikkerheden skal ske uden unødig forsinkelse og om muligt indenfor 24 timer, er for kort frist. Landbrug & Fødevarer er enig i, at brud bør anmeldes uden unødig forsinkelse, men mener ikke at 24 timer er en realistisk tidsramme til sammenligning af, hvornår anmeldelsen er sket uden unødig forsinkelse. Landbrug & Fødevarer mener derfor, at rammen på 24 timer bør fjernes fra bestemmelsen.

Art. 35

Landbrug & Fødevarer mener overordnet, at det synes unødigt byrdefuldt at pålægge større virksomheder at udpege en databeskyttelsesansvarlig. Landbrug & Fødevarer finder, at de opgaver og ansvar, som forordningen på sigt vil pålægge virksomhederne, må være nok til at opfylde forordningens beskyttelseshensyn, uden at der udpeges en bestemt ansvarlig.

Særligt, at vedkommende skal udpeges for en 2-årig periode kan forekomme generende for virksomhedens drift og unødigt byrdefuldt.

Art. 79

Landbrug & Fødevarer finder, at det fastsatte bødeniveau er helt ude af proportioner i forhold til en eventuel tilsigtet eller utilsigtet overtrædelse af reglerne. Landbrug & Fødevarer anbefaler, at niveauet tilpasses medlemslandenes nationale niveau.

Landbrug & Fødevarer efterlyser ligeledes en fleksibilitet i bødeniveauet. I forordningens nuværende udformning er bødeniveauet fastsat, således der ikke er mulighed for at variere bødens størrelse alt efter forseelsens grovhed, skadevirkning, karakter, tidsmæssige varighed og andre lignende individuelle hensyn, som skal indgå i prøvelsen.

Landbrug & Fødevarer finder det betænkeligt, at der gives adgange til administrative bøder på dette område, da der i det administrative system ikke kan gennemføres samme bevisvurdering som ved domstolene, og Landbrug & Fødevarer opfordrer derfor til at bøder – i hvert tilfælde i det foreslåede niveau - kun kan idømmes ved domstolene. Herved indrømmes tilsynsmyndigheden alene adgang til at pålægge administrative bøder for de mindre forseelser, og der bliver idømt et markant mindre bødeniveau i det tilfælde.

Landbrug & Fødevarer er uforstående overfor behovet for at pålægge medlemsstaterne at idømme så høje bøder i forbindelse med lanceringen af forordningen, da man endnu ikke har erfaringer med hvilke gråzoner, der vanskeliggør efterlevelsen af forordningen. Det er Landbrug & Fødevarers vurdering, at man i stedet med fordel kunne evaluere håndhævelsen af forordningens præceptive regler på baggrund af en periode på 2 år.

Med venlig hilsen

Hannah Schmidt Aaes
Juridisk Konsulent

Erhvervspolitik

D +45 3339 4510
M +45 3017 8892
E hsa@lf.dk

DI ITEK

29. juni 2012
HEM

Justitsministeriet
Att.: Fuldmægtig Christian Wiese Svanberg
Slotsholmsgade 10
1216 København K

Danish ICT and Electronics Federation

Høringssvar vedrørende EU Kommissionens nye databeskyttelsesregler

DI og DI ITEK takker for muligheden for at afgive høringssvar til Europa Kommissionens forslag om "om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)". DI og DI ITEK har i den forbindelse følgende bemærkninger.

Baggrund

Privatlivets fred (herefter privacy) er en af de vigtigste parametre i forhold til at sikre, at den europæiske befolkning i deres roller som bl.a. borgere og forbrugere kan have tillid til anvendelsen af digitale tjenester. DI og DI ITEK har derfor gennem de seneste fem år arbejdet ihærdigt for at få sat fokus på beskyttelse af privacy.

Privacy er sikkerhed set fra individets synspunkt. Privacy handler om, at mennesker i videst muligt omfang selv har kontrol over deres data. Og i de tilfælde, hvor det er nødvendigt at afgive data, at sikre, at data beskyttes i tilstrækkeligt omfang.

Privacy handler også om, at mennesker skal have mulighed for at vælge de serviceprovidere, de ud fra deres eget subjektive og informerede valg har tillid til. Det er derfor vigtigt, at borgerne ikke bindes op på monopollignende løsninger, som de ikke selv frivilligt ville vælge. I denne optik handler privacy også om at skabe forudsætninger for konkurrence mellem serviceprovidere.

Hvis vi ikke formår at skabe en situation, hvor den europæiske befolkning (fortsat) kan have tillid til de digitale tjenester, kan vi ikke høste gevinsterne ved at effektivisere vores samfund gennem anvendelse af it, vi kan ikke sikre en sund konkurrence på tværs af de europæiske lande, og vi kan ikke sikre et fortsat optag af nye digitale services og produkter.

Postadresse/Postal address
1787 København V
Danmark
(+45) 3377 3377
itek@di.dk
itek.di.dk

Besøgsadresser/Visiting addresses
Hannemanns Allé 25
København S
Sundkrogskaj 20
København Ø

CVR: 16 07 75 93

Både den offentlige og den private sektor har en rolle at spille for at skabe den fornødne tillid. Hvis tilliden falder til anvendelse af it på det private marked, vil dette have en effekt i forhold til anvendelsen af offentlige digitale services. Hvis ikke der er tillid til anvendelsen af offentlige digitale services, tør den europæiske befolkning heller ikke anvende private tjenester. Der er derfor behov for en indsats fra såvel den offentlige som private sektor på dette område: den offentlige og private sektor må trække på samme hammel.

Forordningen – overordnede positive kommentarer

DI og DI ITEK har med stor tilfredshed noteret sig Kommissionens udspil til ny forordning. I vores optik er der overordnet tale om et udspil præget af ønsket om at skabe tillid hos den europæiske befolkning. Der er taget hensyn til en tiltrængt harmonisering af europæisk lovgivning, der er taget hensyn til nye rettigheder for befolkningen, som afspejler den digitale tidsalder, vi nu lever i, og endelig er der taget højde for behovet for, at den private sektor får nogle administrative lettelser og i stedet for bureaukratiske formalistiske krav faktisk kan gøre en indsats, som reelt forbedrer befolkningens privacy. Der er på disse tre punkter behov for et opgør med den eksisterende databeskyttelsespraksis i Danmark (og Europa), som må anses for at være forældet.

På det helt overordnede plan er DI og DI ITEK derfor meget tilfredse med det nuværende udspil.

DI og DI ITEK er på et overordnet niveau særligt tilfredse med:

- at der er lagt stor vægt på øget harmonisering af reglerne blandt de europæiske lande. For at nå dette mål er det positivt, at der er tale om en forordning. Det er også positivt, at der introduceres en konsistensmekanisme for de nationale datatilsyn (herefter DPA), og at der sikres koordination gennem datatilsynenes samarbejde i European Data Protection Board (herefter EDPB)
- at der er langt op til, at den enkelte virksomhed fremover kun skal referere til eet europæisk datatilsyn i stedet for et datatilsyn i hvert land med forskellige nationale sagsgange og fortolkninger af det eksisterende direktiv
- at anmeldelsespligten til nationale DPA fjernes. Anmeldelsespligten har gennem lang tid været en forsinkende faktor for indførelse af ny teknologi. De nationale DPA'er har haft en urimelig lang sagsbehandlingstid, og det er tvivlsomt, hvilken effekt det har haft på den reelle beskyttelse af befolkningernes data, at DPA'en skulle godkende en it-løsning, inden den kunne tages i brug. Med forslagene i den nye forordning kan indsatsen (og omkostningerne) anvendes på tiltag, der i langt højere grad kan give en reel beskyttelse af privacy som f.eks. Data Protection Impact Assessment (herefter DPIA), Privacy by Design and Default (herefter PbDx2) og bedre sikkerhed f.eks. i form af Privacy Enhancing Technologies (herefter PET)
- at der fjernes andre administrative byrder end anmeldelsespligten

- at tilliden til digitale tjenester ser ud til at kunne forbedres gennem fastholdelse af eksisterende rettigheder (f.eks. princippet om dataminimering og formålsspecificering), introduktion af nye rettigheder for borgerne (f.eks. retten til at blive glemt, lettere adgang til oversigt over hvad der er gemt af data, ret til data portablitet, retten til ikke at blive profileret og mere information generelt) samt introduktion af nye relevante krav til "processor" og "controller" (f.eks. PbDx2, DPIA, PET, kontaktpunkt hos Data Protection Officer (herefter DPO))
- at der er tiltag til at lette overførelsen af data til tredjelande gennem introduktionen af en flerhed af forskellige muligheder f.eks. "adequacy decisions", "Binding Corporate Rules" (herefter BCR) og "standard clauses" uden DPA godkendelse.

Det er vigtigt, at der fra dansk side arbejdes for, at disse tiltag ikke udvandes i de europæiske politiske forhandlinger.

Forordningen – overordnede negative kommentarer

DI og DI ITEK er imidlertid af den opfattelse, at ikke alle forhold i forordningen er positive. Der er behov for justeringer – særligt i forhold til forholdet mellem "controller" og "processor" samt i forhold til det arbejdsretlige område. På overoverordnet plan har vi nedenstående bemærkninger. I næste afsnit følger detaljerede bemærkninger og rettelsesforslag til de enkelte artikler:

- For det første bør det sikres, at frivillige overenskomster og andre frivillige aftaler på arbejdsmarkedet sidestilles med lovgivningen, således at den nuværende danske retsstilling opretholdes. Tilsvarende er det også vigtigt, at ledelsesretten også i fremtiden kan finde anvendelse. Særligt må arbejdsgiver også i fremtiden have mulighed for under samtykke med arbejdstager, at behandle personlige data om vedkommende. Yderligere må arbejdsgiver have ret til at kunne kræve lægeerklæring og straffeattest fra arbejdstager. Der henvises til de uddybende kommentarer nedenfor - særligt Artikel 7, stk. 4; Artikel 9 stk. 2, litra b, d og j; Artikel 21, stk. 1 (nyt litra), Artikel 81 og Artikel 82.
- For det andet bør forholdet mellem den dataansvarlige (registeransvarlig) (herefter controller) og databehandleren (registerfører) (herefter processor) præciseres. Ifølge den eksisterende lovgivning er controlleren alene ansvarlig. Der findes i forordningen et markant opgør med dette princip idet ansvaret deles mellem controller og processor og dermed pålægger ansvar til processor i den eksisterende lovgivning. DI og DI ITEK mener, at det er uhensigtsmæssigt og farligt at dele ansvaret, idet ansvaret så reelt enten kan falde mellem to stole eller skabe uoverensstemmelse mellem controller og processor om, hvem der har ansvaret for hvad. DI og DI ITEK anbefaler, at det forsat alene er controller, der har det endelige ansvar for behandlingen af data overfor såvel myndigheder som de registrerede. Ansvarsfordelingen mellem controller og processor bør overlades til

aftalemæssig regulering mellem controller og processor, således at ansvaret inter partes kan placeres, hvor parterne finder det mest hensigtsmæssigt, uden at dette påvirker controllerens placering som pligtsubjekt overfor myndigheder og de registrerede. Dette kan f.eks. ske ved at controller stiller krav til processor f.eks. med hensyn til videreoutsourcing, kontrol (kapacitet, evne, risikovurdering og passende foranstaltninger), afgrænsning, kvalitet, kvantitet, fejl og tid, som vi kender det fra den finansielle sektor og "Bekendtgørelse om outsourcing af væsentlige aktivitetsområder". DI og DI ITEK anbefaler dog, at det vurderes, om der kan introduceres et ansvar for processor til at fortælle controller om aktuelle sikkerhedsforanstaltninger og teknologiske forhold, som det må forventes at processor har en bedre forudsætning for at have viden om end controller. Det kan f.eks. være informationer om, hvordan man designer sin arkitektur så PbDx2 er opfyldt, hvordan man implementerer sikkerhed i form af kryptering, logning m.v., og hvordan man introducerer PET - herunder især enabler befolkningen til bedst muligt at beskytte deres egne informationer. Desuden skal der naturligvis være en kontrakt mellem de to parter, som der også er lagt op til i Forordningen, og som det kendes fra den eksisterende lovgivning.

- For det tredje er det urealistisk og fagligt uforsvarligt, at der, hvor muligt, skal laves en omfattende "data breach notification" indenfor 24 timer. En sådan notificering er ikke rimelig eller mulig, da der typisk ikke kan skabes et fornødent overblik indenfor en så kort tidshorisont, ligesom tidshorisonten ikke vil give controlleren tid til at foretage de nødvendige modforanstaltninger, inden bruddet offentliggøres. Vi forudser, at såfremt der tilstræbes informationer med så kort varsel, vil der i mange tilfælde blive behov for at komme med berigtigelser til de først fremkomne informationer, i takt med at man får mere viden om databruddet. Dette vil ikke bidrage til at øge tilliden til it-løsningerne - tværtimod vil det udvande tilliden. Vi ønsker, at bemærkningen om de 24 timer helt fjernes. Mere overordnet stiller DI og DI ITEK sig generelt tvivlende overfor det formålstjenelige ved en sådan notificering, idet dette vil kræve signifikante ressourcer hos såvel virksomhederne som DPA'erne, uden at der synes at være sammenhæng mellem den betragtelige forøgede administrative byrde og fordelene ved sådan en notificering
- For det fjerde er der lagt op til helt uacceptable administrative bøder, som er ude af proportioner med de fejl, som controller eller processor måtte have begået. Den nuværende bødestruktur og de nuværende bødestørrelser skaber incitament for DPA'erne til alene at fokusere på brud i virksomheder, som er ejet af store internationale koncerner, fordi de herfra kan indhente de største beløb uden at dette nødvendigvis er en reel afspejling af, hvor de største risici for overtrædelser ligger. Derudover pålægges bøderne også for simple uagtsomme handlinger eller undladelser, hvilket igen fremstår uproportionalt. Herudover bør bøderne afspejle forholdets grovhed, herunder om der er tale om systematiske og/eller forsætlige overtrædelser, mens der må bibeholdes en mulighed for at lade uagtsomme overtrædelser være genstand for administrative advarsler. Det

skal i denne sammenhæng bemærkes, at hvor bøder under konkurrencelovgivningen er baseret på økonomiske beregninger af den antikompetitive skadesvirkning, gør dette sig ikke gældende for brud på privacylovgivningen, hvorfor den omsætningsmæssige bødeudregning synes uproportional. Yderligere vil et prohibitivt bødeniveau som foreslået kunne bremse den digitale udvikling i Europa, i det virksomheder kan vælge at afstå fra opgaven alene grundet den ekstremt høje finansielle risiko ved disse bødestørrelser. DI og DI ITEK anbefaler, at bøderne beregnes alene ud fra det enkelte selskab, der har begået fejl i forbindelse med overholdelse af lovgivningen og ikke ud fra den koncern selskabet indgår i. Desuden anbefaler DI og DI ITEK, at bødernes størrelse reduceres til en faktor gange et skøn af de omkostninger, virksomhederne har sparet ved ikke at indføre beskyttende tiltag plus de økonomiske gevinster som de manglende beskyttende tiltag måtte have givet. De skader, der er forvoldt ved den manglende beskyttelse, bør også have en betydning.

- DI og DI ITEK er som tidligere anført principielt tilhængere af de fleste af de øvrige nye initiativer der introduceres med forordningen – herunder bl.a. DPIA, PbDx2, PET og DPO. Det er imidlertid vigtigt, at der henses til, hvor store de administrative omkostninger bliver, i forhold til hvad der kan spares af andre veje, så vi ikke underminerer europæisk konkurrenceevne.
- Europa har bedre beskyttelse af privacy end mange andre steder i verden. Det er imidlertid vigtigt, at man i Europa skeler til privacy fremmende initiativer udenfor Europa og lader sig inspirere, så vi ikke låser os inde i Europa. Særligt hvor der findes globale standarder, f.eks. ISO/IEC JTC 1/SC 27, bør man benytte disse. I forhold til at etablere mærkningsordninger vil det være nyttigt at se, om man kan samarbejde udenfor Europa – f.eks. med TRUSTe.
- Der er i forslaget meget få sondringer mellem, i hvilket omfang forskellige typer af data bør beskyttes afhængig af om data er følsomme eller ej. En lang række data må slet ikke behandles, med mindre der er særlige omstændigheder. Andre data skal beskyttes lige godt, uanset om de er tale om almindelige oplysninger som f.eks. en adresse eller følsomme/fortrolige oplysninger om f.eks. helbred eller strafbare forhold. Vi vil gerne opfordre til, at der i langt højere grad indarbejdes en graduering af kravene i forhold til beskyttelseshensynene. Således vil det være nyttigt at arbejde mere med at fastsætte forskellige beskyttelseskrav til forskellige typer af data. F.eks. bør dokumentationen omtalt i artikel 28 stk. 2, litra d, ikke være lige så omfattende for adresser som for genetiske data. Som et andet eksempel må kontaktinformation på medarbejdere i deres professionelle sammenhæng (business contact information) ikke påkalde sig beskyttelse som persondata, da der ikke synes at være noget særskilt beskyttelseshensyn overfor sådanne data, som typisk vil være offentligt tilgængelige på f.eks. hjemmeside eller visitkort. DI og DI ITEK anbefaler, at data beskyttes ud fra en risikobetragtning således, at de mest følsomme data beskyttes bedst. En sådan tilgang vil ikke indebære en forringelse af beskyttelsen, hvor denne er af betydning, men ville omvendt

understøtte formålet om administrative lettelser for virksomheder. Det ville samtidig sikre en generel bedre forståelse og accept af de lovgivningsmæssige krav og imødegå den udbredte opfattelse i virksomheder, at reglerne mest af alt er tunge administrative byrder.

- Endvidere anbefales det, at det konkretiseres specifikt, hvilke typer af data, der skal betragtes som følsomme, fortrolige, etc. i relation til virksomhedernes registrering og behandling af disse. Det er svært håndterbart rent operationelt, at datatype A er fortrolig/følsom i situation 1, mens datatype A ikke er det i situation 2.
- Det er bekymrende, at Kommissionen i så stort omfang (26 steder), som skitseret, lægger op til at bruge "delegated acts" (delegerede retsakter), herunder på betydelige områder som f.eks. artikel 6.5, 9.3, 33.4, 26.5 og 28.5. På den ene side er det glædeligt, at der arbejdes på at opnå større harmonisering. På den anden side er det demokratiske element i delegated acts lille og beslutningsproceduren for delegated acts ret uigennemskuelig. Anvendelsen af delegerede retsakter kan også skabe usikkerhed omkring forudsigeligheden af reglerne og dermed virksomhedernes mulighed for at indrette sig i overensstemmelse med lovgivningen tillige med deres omkostninger og konkurrenceevne. DI og DI ITEK foreslår, at omfanget af delegated acts vurderes igen. Desuden bør det sikres, at relevante interessenter - herunder industri og forbrugere - høres, og at der ved retsaktens udarbejdelse inddrages uafhængige (gerne forskningsbaserede) vurderinger af tekniske muligheder og vanskeligheder samt økonomiske konsekvenser. DI og DI ITEK foreslår desuden, at der skal ske en obligatorisk evaluering af anvendelsen af enhver delegated act to år efter dens vedtagelse, hvor retsakten vurderes ud fra dens formål, dens grad af understøttelse af harmonisering indenfor EU, teknologiens aktuelle stade og de økonomiske byrder. Evalueringen skal være underlagt demokratisk politisk kontrol og desuden skal relevante parter - herunder industri og forbrugere - høres.

Forordningen – detaljerede kommentarer

Foruden de overordnede kommentarer ovenfor, har DI og DI ITEK en række mere detaljerede kommentarer til de enkelte artikler i forordningen.

Kapitel I – Generelle bestemmelser

- Artikel 2, stk. 2, litra b: DI og DI ITEK finder, at det er uhensigtsmæssigt, at forordningen ikke gælder for EU-institutioner, -organer, -kontorer og –agenturers behandling af personoplysninger. Der synes ikke at være nogen grund til at undtage disse. Borgerne bør kunne være sikre på, at deres persondata er underlagt den samme beskyttelse uafhængigt af, hvem der behandler deres data. DI og DI ITEK anbefaler, at litra b udgår. At samme årsager er DI og DI ITEK også skeptisk overfor fastholdelse af litra a) og litra e). Det bør i bemærkningerne til loven fremgå, hvorfor der skal opretholdes

undtagelser for så bredt et begreb som "national sikkerhed" og desuden for retsvæsenet.

- Artikel 4, 1): Under omtalen, af hvad der kan anvendes til at identificere en "registreret", er begrebet "lokaliseringsdata" problematisk. Lokaliseringsdata siger noget om, hvor en enhed befinder sig, men siger ikke noget om, hvem der bærer enheden. For det første er det generelt problematisk at henføre "lokaliseringsdata" til en "registreret", idet dette vil umuliggøre mange potentielle fremtidige services rettet mod europæiske borgere. For det andet kan anvendelsen af begrebet "lokaliseringsdata" betyde, at den måde hele mobiltefoniinfrastrukturen fungerer på, skal ændres, med kæmpe omkostninger for de europæiske mobilkunder. For det tredje vil en henføring af "lokaliseringsdata" til en "registreret" formodentlig betyde, at logningsbekendtgørelsen ikke kan opretholdes. DI og DI ITEK anbefaler, at "lokaliseringsdata" udgår. Subsidiært at begrebet defineres selvstændigt i artikel 4 i lyset af de ovenstående bemærkninger. Anonymisering af data og anonyme data (herunder data som er indirekte identificerbare men hvor identifikationsnøglen ikke medfølger) bør eksplicit undtages fra henholdsvis behandlingsbegrebet og persondata definitionen. Herudover er det uklart, hvad der menes med at personen er "indirectly identifiable", og der bør opsættes kriterier herfor som vejledning.
- Artikel 4, 2): Definitionen af personoplysninger (navnlig når den ses i sammenhæng med artikel 4, 1)) synes i sin nuværende formulering at inkludere kontaktinformationer på medarbejdere i deres professionelle kapacitet – altså navn, jobrolle og –titel samt arbejdskontaktoplysninger (arbejdsemail, -telefonnummer, -faxnummer, -postadresse, og –besøgsadresse) også kaldet "business contact information". Det er DI og DI ITEKs opfattelse, at disse informationer bør undtages definitionen, således som det spanske datatilsyn allerede har fortolket den nuværende lovgivning. Der synes ikke at være noget beskyttelseshensyn for sådan information, og en undtagelse vil lette behandlingen af disse oplysninger. Oplysningerne har generelt et formål, der adresserer virksomheden og ikke personen. Der kan opsættes begrænsninger på at sådanne oplysninger alene er undtaget, forudsat at behandlingen begrænses til det nødvendige i forretningsmæssige sammenhænge.
- Artikel 4, 5) og artikel 4, 6): Processor og controller er ikke tilstrækkeligt tydeligt defineret. Det fremgår ikke af de nuværende definitioner, om virksomheder som f.eks. Google eller Facebook, er det ene eller det andet eller begge dele afhængigt den konkrete behandling. Det vil derfor være vanskeligt for virksomheder og myndigheder at vurdere, hvornår de har hvilken rolle. I visse sammenhænge kan det også ske, at den registrerede selv optræder som controller og processor af data - og selv behandler data så de offentliggøres via en tjeneste. DI og DI ITEK anbefaler tydeligere definitioner. DI og DI ITEK anbefaler desuden, at der som et led i harmoniseringen udarbejdes eksempler, som letter beslutningen for virksomheder og myndigheder i at vurdere, hvornår de har hvilken rolle.
- Artikel 4, 8): Definitionen af samtykke synes at være i overensstemmelse med den danske praksis for fortolkning af begrebet - herunder elementet

"udtrykkelig". Det fortolkning synes også at have bred politisk opbakning i lyset af "cookie reguleringen". Imidlertid er dette ikke for nuværende en fortolkning, der gør sig gældende i alle EU-lande. DI og DI ITEK ønsker, at det lægges vægt på en harmoniseret fortolkning på tværs af alle EU-lande. Herudover bør der redegøres for, hvorledes denne klargøring påvirker de danske regler i Markedsføringslovens §6, stk. 2 og 3, idet disse synes at fungere tilfredsstillende med muligheden for at "opt out" af evt. henvendelser.

- Artikel 4, 9): Definitionen af "personal data breach" er ikke baseret på, hvorvidt en breach rent faktisk afstedkommer en risiko for skade på individer, f.eks. hvor breachen alene vedrører krypteret data. DI og DI ITEK opfordrer til, at alene breaches, hvori der består en aktuel risiko for kompromittering af data, betragtes som en "personal data breach".

Kapitel II - Principper

- Artikel 5(f): DI og DI ITEK har noteret sig, at artikel 5(f) tydeligt angiver, at ansvaret for behandlingen påhviler den dataansvarlige. Dette klare ansvar reflekteres dog ikke i andre artikler (for eksempel artikel 26, 31 og 34, 1. afsnit), hvor processors ansvar beskrives. Der bør i den endelige forordning være en klokkeklar beskrivelse af ansvarområdet.
- Artikel 6, stk. 1, litra d: "behandling... i samfundets interesse eller henhørende under offentlig myndighedsudøvelse" er en meget vid definition, som giver brede muligheder for, at den offentlige sektor kan behandle data. Set i sammenhæng med Artikel 6, stk. 3 kan der til enhver tid vedtages national lovgivning, som gennemtvinger ret til behandling af enhver form for persondata. I henhold til stk. 4 kan man endda med udgangspunkt i lovgivning justere formålet for behandling af allerede indsamlede data. DI og DI ITEK vil gerne påpege, at dette omfattende hensyn til national lovgivning betyder, at harmoniseringen af databeskyttelsen i EU vil komme under pres: borgerne i de forskellige EU-lande vil få deres data behandlet forskelligt af deres respektive nationale myndigheder. Dette er utilfredsstillende. DI og DI ITEK ønsker, at bestemmelserne justeres således, at det kun rent undtagelsesvist bliver muligt at behandle data med udgangspunkt i national særlovgivning. I tilknytning hertil skal det understreges, at selv når denne undtagelse finder anvendelse skal behandlingen ske i overensstemmelse med Forordningens regler. Tilsvarende betragtninger gælder for litra c om "retlige forpligtelser". Se også kommentarer til Artikel 21.
- Artikel 7, stk. 4 (og præambel 34): DI og DI ITEK er principielt tilhænger af at samtykke - selv for almindelige personoplysninger - ikke kan tilvejebringe et retsgrundlag for behandling, hvor der kan være berettiget tvivl om hvorvidt samtykket har været frivilligt. Bestemmelsen, om at samtykket ikke er gyldigt", hvis der er en klar skævhed mellem den registrerede og den registeransvarlige" ("significant imbalance") giver dog anledning til betydelig fortolkningstvivl og er vanskelig anvendelig i praksis. DI og DI ITEK foreslår derfor primært, at man bibeholder principperne om, at samtykket skal være frivilligt, men at kravet om "ingen skævhed" slettes, ligesom præambel

34 slettes, da frivillighedskravet er bærer af de samme hensyn som kravet om "ingen skævhed". Såfremt "ingen skævhed" ikke kan fjernes fra artiklen, er det DI og DI ITEKs opfattelse, at der skal indføres en undtagelse for arbejdsmarkedets parter. Det er centralt, at arbejdsgiver kan behandle visse oplysninger om medarbejderne med deres samtykke, herunder på medarbejderens initiativ, desuagtet at der kan anses at være en skævhed i forholdet mellem arbejdstager og arbejdsgiver. DI og DI ITEK anbefaler derfor subsidiært, at der tilføjes et stk. 5, hvor det præciseres: "Stk. 4 finder ikke anvendelse i forholdet mellem arbejdsgiver og arbejdstager." Om flere kommentarer i forholdet mellem arbejdsgiver og arbejdstager henvises der bl.a. til kommentarer til artikel 82.

- Artikel 9, stk. 1: I følge den gældende danske fortolkning af det gældende direktiv har vi i Danmark særlig beskyttelse af visse kategorier af data kaldet semi-følsomme oplysninger (Lov om behandling af personoplysninger §8). Der er tale om "strafbare forhold, væsentlige sociale problemer og andre rent private forhold". DI og DI ITEK anbefaler, at disse kategorier af data tilføjes Artikel 9. Således bør Artikel 9, stk. 1 hvad angår kategorier af data afspejle den gældende Lov om behandling af personoplysninger §§ 7 og 8.
  Endvidere anbefales det, at det konkretiseres specifikt hvilke typer data, der skal betragtes som følsomme, fortrolige etc. i relation til virksomheders registrering og behandling af disse. Det er svært håndterbart rent operationelt, at datatype A er fortrolig/følsom i situation 1, mens datatype A ikke er det i situation 2.
- Artikel 9, stk. 2, litra b: Det bør afklares i hvilket omfang behandling af følsomme data, som er omfattet i aftaler mellem arbejdsmarkedets parter, og som ikke er vedtaget ved lov, er undtaget fra behandling. DI og DI ITEK anbefaler, at kollektive overenskomster og kollektive aftaler på arbejdsmarkedet sidestilles med loven, således at ordlyd bliver: "... hjemlet i EU-retten, medlemsstatens lovgivning eller aftale mellem arbejdsmarkedets parter...". Det er helt centralt for arbejdsgivere og arbejdstagere, at der fortsat kan behandles oplysninger om fagforeningsmæssigt tilhørsforhold, helbredsoplysninger, personlighedstests og straffeerklæringer.
- Artikel 9, stk. 2, litra d: I den eksisterende danske lovgivning kan arbejdsmarkedets organisationer behandle disse data og desuden jf. § 49, stk. 3 undlade at foretage anmeldelse til DPA. Det er DI og DI ITEKs forudsætning, at fortolkningen af Forordningen giver anledning til uændret retspraksis på dette område.
- Artikel 9, stk. 2, litra j: Behandling af personoplysninger vedrørende straffedomme m.v. kan være nødvendigt for arbejdsgiver i vurdering af en nuværende eller potentielt kommende arbejdstager. DI og DI ITEK ønsker, at der i litra j eksplicit gøres opmærksom på, at arbejdsgiver skal kunne indhente straffeattester.

Kapitel III – Den registrerede rettigheder

- Artikel 14-19: Det stilles ikke krav til, hvordan den registrerede skal dokumentere sin identitet og dermed kunne udøve sin ret til at få indsigt i data, rettet data, slettet data eller porteret data. Såfremt denne identitet ikke dokumenteres tilstrækkeligt grundigt, vil de nye gode rettigheder borgerne tilføres kunne misbruges til at stjæle personoplysninger fra andre – og i særligt grelle tilfælde identiteter – eller på anden måde ødelægge andres identitet på internettet i stor stil. DI og DI ITEK anbefaler, at der stilles krav til, hvordan den registrerede skal dokumentere sin identitet.
- Artikel 17, stk. 2: Der henvises i forbindelse med The Right to be Forgotten til "...rimelige foranstaltninger, herunder tekniske foranstaltninger, vedrørende oplysninger,..., for at underrette tredjeparter,..., om, at en registreret ønsker at de sletter...", som controlleren skal tage. I denne formulering er der flere uklare forhold. For det første specificeres det ikke, hvad rimelige foranstaltninger er. For det andet specificeres det ikke, hvilke tekniske foranstaltninger der tænkes på. For det tredje er det uklart, hvad underretning indebærer af konsekvenser for tredjepart.
  DI og DI ITEK foreslår, at artiklen rettes således, at forpligtelsen for controller i de tilfælde, hvor der ikke foreligger kontrakt mellem controller og tredjepart, og hvor der modtages en henvendelse fra den registrerede, begrænses til at rette henvendelse til tredjepart (hvor tredjepart er kendt) og bede om, at data slettes, alternativt at anmodning om sletning offentliggøres. Det kan efter en sådan henvendelse evt. overvejes, om tredjepart herefter skal betragtes som controller.
  DI og DI ITEK foreslår desuden, at de data, der skal slettes, hvad enten data befinder sig hos controller eller processor, og uanset om der foreligger kontrakt mellem parterne eller ej, alene er data, som er umiddelbart tilgængelige. Herunder skal ikke omfattes anonymiserede data eller data på backup. Der bør i denne forbindelse eksplicit henvises til undtagelsen i artikel 10. DI og DI ITEK skal bemærke, at vi principielt tilhængere af "Retten til at blive glemt". Vi er dog skeptiske overfor, hvorledes dette kan implementeres i praksis. Man skal være opmærksom på at data, der f.eks. af den registrerede selv er gjort tilgængelige på visse hjemmesider på internettet, kan være kopieret af tredjemand, og derfor vil være umulige at få slettet.
- Artikel 18: DI og DI ITEK er principielt tilhængere af, at det gøres let at portere data mellem tjenester. Det er dog centralt, at der fra Kommissionens side henvises til internationale standarder på området. Det er også centralt, at der skeles til, at europæiske serviceudbydere ikke stilles ringere end serviceudbydere udenfor EU.
- Artikel 20 (og præambel 58): DI og DI ITEK er principielt tilhængere af, at der ikke skal kunne foretages unødig behandling, herunder profilering - særligt ikke uden de registreredes vidende - jf. stk. 1. Dette forhold er andre steder bl.a. adresseret i "cookie-reguleringen", hvor der ikke må placeres kode på brugernes terminaludstyr, fordi man fra politisk side har ønsket at forhindre overvågning af brugernes adfærd på nettet - herunder deres præferencer. Imidlertid noterer DI og DI ITEK sig, at bestemmelsen i Artikel 20 er

ret bred. Der er derfor behov for, at man gennem praksis eller de delegerede retsakter i omtalt i stk. 5, lægger op til en lige så bred anvendelse af undtagelsesbestemmelserne i stk. 2. F.eks. kan forsikringsselskaber eller analysebureauer have behov for at have en vis viden om de registrerede for at kunne drive deres virksomhed.

- Artikel 21: Undtagelsesbestemmelser i denne artikel er ligesom undtagelserne i Artikel 6, stk. 1, litra d meget brede. DI og DI ITEK vil gerne påpege, at dette omfattende hensyn til nationale forhold betyder, at harmoniseringen af databeskyttelsen i EU vil komme under pres: borgerne i de forskellige EU-lande vil få deres data behandlet forskelligt af deres respektive nationale myndigheder. Dette er særligt et problem i forhold til den offentlige sektors behandling af data. DI og DI ITEK ønsker, at bestemmelserne justeres således, at det kun rent undtagelsesvist bliver muligt at behandle data med udgangspunkt i særlige nationale hensyn. DI og DI ITEK har bemærket, at the European Data Protection Supervisor (herefter EDPS) ligesom DI og DI ITEK retter en kritik af disse vide bestemmelser. DI og DI ITEK anbefaler at der igangsættes en dialog med EDPS om, hvordan undtagelserne kan indsnævres, og hvordan man kan stille krav til kvaliteten of formålet i den nationale lovgivning.
  På det danske arbejdsmarked er det dog indlysende, at vi ikke vil kunne fortsætte med at løse forholdende mellem arbejdsmarkedets parter, såfremt bestemmelsen opretholdes i sin nuværende form. Det vil medføre uhyrlige administrative omkostninger for arbejdsgiverne såfremt artiklerne 11-20 skal opretholdes mellem arbejdsmarkedets parter. Det synes heller ikke at være lovens formål, at loven skal finde anvendelse på dette område. DI og DI ITEK skal derfor på det kraftigste anbefale, at der indføres et nyt stk. 1, litra g, som eksplicit undtager forholdet mellem arbejdsgiver og arbejdstager.

Kapitel IV – Registeransvarlig og registerfører

- Artikel 22 og Artikel 26, m.fl. (bl.a. artikel 28, 33, 34 og 77) (om forholdet mellem controller og processor): Der lægges i den nye forordning op til en ansvarsfordeling mellem controller og processer. Det er dog uklart, i hvilket omfang der er tale om et egentligt "ansvar" idet ordene "ansvar" og "forpligtelser" anvendes i flæng (3.4.4.1, p.10 og (62), p. 28). Det er også uklart, om det er controller eller processor, der er ansvarlig for dokumentation og samarbejde med DPA ((65), p. 29). Dette er ikke hensigtsmæssigt, da et delt ansvar falder mellem to stole. Det er især ikke hensigtsmæssigt i lyset af definitionerne – jf. kommentarerne til artikel 4, 5) og 6). Det er desuden uklart, hvad der skal til af behandling, for at processor kan antages at indtage rollen som controller i medfør af artikel 26, stk. 4. DI og DI ITEK anbefaler, som tidligere nævnt, at det nugældende princip med ansvar placeret hos controller opretholdes. Det nytter ikke noget, at en processor kan gøres ansvarlig for f.eks. ikke at have leveret en privacy forbedrende service, som controlleren ikke ville købe. Risikofordelingen mellem parterne bør reguleres af markedet. Forholdet mellem de to parter og deres respektive forpligtelser

bør fastlægges i en kontrakt, som parterne er enige om. Der kan så i forordningen stilles overordnede krav til indholdet af kontrakten, f.eks. således at den viden om mulige tekniske løsninger - f.eks. kryptering, pseudonymisering og styring af privacy via policies - obligatorisk stilles til rådighed for controlleren af processoren. Kontrakten skal i lighed med praksis fra den finansielle sektors "Bekendtgørelse om outsourcing af væsentlige aktivitetsområder" stille krav til bl.a. videreoutsourcing, kontrol (kapacitet, evne, risikovurdering og passende foranstaltninger), afgrænsning, kvalitet, kvantitet, fejl og tid.

- Artikel 23: DI og DI ITEK er principielt set tilhænger af, at privacy designes ind i systemer og slås til som standard (PbDx2). Vi håber, at denne artikel kan give anledning til at der udvikles og implementeres nye teknologiske metoder til beskyttelse af privacy, som f.eks. pseudonymisering og transaktionsanonymitet. Det er imidlertid vigtigt, at forordningen bliver mere specifik i forhold til, hvordan virksomhederne kan komme i compliance med denne artikel. Den nuværende beskrivelse er ganske uklar, da især design elementet er meget situationsbestemt. Samtidig er det vigtigt, at kravene får en form, hvor der er tale om teknologineutralitet.
- Artikel 26, stk. 3: Det er vigtigt, at der er en fælles forståelse af samarbejdet mellem processor og controller. Det fremgår ikke tydeligt, at den skriftlige dokumentation af controllers instrukser og processors forpligtelser skal være eet og samme dokument. Hvis dette ikke er tilfældet, kan de to parter have forskellige opfattelser af, hvad der kræves af den anden part. I øvrigt er det at betragte som en administrativ byrde uden positiv effekt for beskyttelsen af data at kræve to dokumenter. DI og DI ITEK anbefaler derfor, at det præciseres, at der kun forefindes eet sæt dokumentation.
- Artikel 28: Som følge af bemærkninger til artikel 22 og 26 anbefaler DI, at der alene henvises til at controller har ansvaret for dokumentation.
- Artikel 31: Generelt er der grund til at være skeptisk i forhold til notifikation af brud på persondatasikkerheden. I de fleste tilfælde vil det kun være de controllere/processorer, som har godt styr på sikkerheden, der overhovedet vil opdage, at der er sket et brud. Dette giver en asymmetri i forhold til hvilke tilfælde, der bliver notificeret. Desuden vil det ikke nødvendigvis forbedre sikkerheden at notificere alting – i stedet vil det bare skabe ligegyldighed overfor sikkerhedsbrud blandt visse samfundsgrupper og ekstra frygt for at anvende digitale tjenester blandt andre samfundsgrupper. Der synes ikke at være sammenhæng mellem den betydelige administrative byrde som pålægges controllerne (og de lokale DPA) og den (begrænsede) beskyttelsesvirkning, som notificeringen vil medføre. DI og DI ITEK anbefaler, at Artikel 31 forkastes i sin helhed. Såfremt det ikke sker, anbefaler DI og DI ITEK som et minimum, at notifikationen alene bringes i anvendelse i de tilfælde, hvor data er af særlig følsom karakter – nemlig data der behandles i henhold til artikel 9, stk. 2 – og at der i sådanne tilfælde gives en hensigtsmæssig notifikationsfrist, således at controlleren har mulighed for at vurdere bruddet, herunder implicerede data og personer, samt tage sikkerhedsmæssige foranstaltninger inden bruddet offentliggøres.

- Artikel 31, stk. 1: Det er i langt de fleste tilfælde ikke muligt at indsamle og indberette alle de i stk. 3 nævnte informationer indenfor 24 timer – og hvis virksomhederne forsøger det, kan det resultere i sjusk og ændringer i informationerne senere i forløbet. Som angivet ovenfor ønsker DI og DI ITEK artikel 31 slettet i sin helhed. Er dette ikke muligt ønsker DI og DI ITEK at henvisningen til 24 slettes og at man alene opretholder "uden unødig forsinkelse".
- Artikel 32: DI og DI ITEK er enige i, at hvor der består en risiko for skade for den registrerede, bør denne som god skik adviseres om brud på persondatasikkerheden. Artikel 32 synes dog ikke at være baseret på nogen vurdering af, hvorvidt der består risiko for skade. For at undgå "notificerings fatigue" hos de registrerede og samtidigt sikre, at den registrerede kan tage de nødvendige forholdsregler, hvor der er risiko for skade, foreslår DI og DI ITEK at notificering alene kræves, hvor der er risiko for skade for den registrerede.
- Artikel 33: DI og DI ITEK har gennem flere år advokeret for anvendelse af Privacy Impact Assessments, der i forordningen er blevet til DPIA. DI og DI ITEK er derfor meget positive overfor, at dette er taget med i udkastet til Forordning og anbefaler at det fastholdes i Forordningen. Det er imidlertid vigtigt at DPIA ikke gøres obligatorisk for alle projekter. DPIA bør anvendes ved særligt kritiske projekter, hvor privacy står overfor særlige risici. DI og DI ITEK har noteret sig betingelser i stk. 2. DI og DI ITEK foreslår imidlertid at der tilføjes et litra f), hvor det fremgår at kritisk infrastruktur komponenter, som anvendes i forbindelse med almindelige eller følsomme data, også underkastes en DPIA. Konkret tænkes der på, at det burde være et lovgivningsmæssigt krav at foretage DPIA i forhold til danske løsninger som f.eks. NemID, e-Boks og NemSMS. DI ITEK foreslår som følge af kommentarer til Artikel 22 og 26 at det præciseres, at det er controllers ansvar at få gennemført en DPIA.
- Artikel 33, stk. 4: DI og DI ITEK er sympatisk overfor brugerinddragelse ved udvikling af it-systemer – specielt med det formål at bedrive brugerdreven innovation. Sådan brugerinddragelse bør dog være drevet af markedskræfterne og egner sig ikke til lovregulering. Herudover kan stk. 4 misbruges til at indhente en blåstempling af en dårlig sikkerhedsløsning fra brugerne, uden at disse har den fornødne indsigt til at vurdere løsningen. Controller kan dermed flygte fra sit ansvar. Effekten af dette initiativ for privatlivsbeskyttelsen er i bedste fald usikker, og det vil derfor i væsentligt omfang være en administrativ byrde. DI og DI ITEK opfordrer til, at stk. 4 udgår i sin helhed.
- Artikel 33, stk. 5: Den offentlige sektor er stadig i besiddelse af langt mere følsomme og detaljerede oplysninger end den private sektor – f.eks. oplysninger om straf og elektroniske patientoplysninger. Derfor forekommer det uproportionalt og uhensigtsmæssigt, at den offentlige sektor ikke skal foretage en konsekvensanalyse vedrørende databeskyttelse i offentlige it-systemer. Ved at opretholde denne paragraf kan medlemsstaterne lovgive sig til dårlig offentlig databeskyttelse - hvad man i praksis sagtens kan forestille

sig ske for at spare penge. DI og DI ITEK opfordrer på det kraftigste til at stk. 5 udgår.

- Artikel 34, stk. 1: Artiklen og dens sammenhæng med artikel 41, stk. 1, artikel 42, stk. 2, litra d, artikel 42, stk. 4 og artikel 42, stk. 5, bør tydeliggøres. Det forekommer uklart, om der skal søges godkendelse for kontraktens indhold, behandlingen og overførslen hver for sig eller om det skal ske samlet. Der forekommer også uklart, om overførslen til tredjelande skal godkendes igen, hvis datakategorierne ændrer sig. DI og DI ITEK anbefaler, at der hurtigst muligt udarbejdes tydelige vejledninger om de forskellige muligheder for at overføre data til tredjelande. DI og DI ITEK foreslår som følge af kommentarerne til Artikel 22 og 26, at det præciseres, at det entydigt er controllers ansvar at få gennemført en godkendelse hos DPA.
- Artikel 35-37: DI og DI ITEK er generelt tilhænger af, at der skal udpeges et kontaktpunkt for databeskyttelse i virksomheden og ser det samtidig som værende fornuftigt, at dette kontaktpunkt løfter forpligtelserne beskrevet i artikel 37. DI og DI ITEK har imidlertid en række reservationer overfor måden, det implementeres på i artiklerne 35-37. Særligt er vi ikke tilfredse med at der peges på, at DPO'en skal være én person.
  For det første synes det ikke rimeligt at virksomhederne pålægges at ansætte en person, for hvem ledelsen ikke har nogen ledelsesret (jf. artikel 36 stk. 2) i form af instruktionsbeføjelser. Hertil kommer at ledelsen heller ikke kan afskedige DPO'en, hvis der opstår samarbejdsvanskeligheder, hyppigt fravær eller andet (jf. artikel 35 stk. 7). Tilsvarende situation ville opstå i forhold til en ekstern serviceleverandør. Det må i højere grad være op til den enkelte virksomhed, hvordan den vil organisere sig og sikre, at kravene fra artikel 37 kan efterleves.
  For det andet vurderer DI og DI ITEK, at forpligtelserne for DPO'en omtalt i artikel 37 er utilstrækkelige. Det er nødvendigt, at kontaktpunktet ikke alene har juridiske kompetencer, men også tekniske kompetencer for at kunne efterleve moderne krav til elektronisk databehandling.
  Af samme grund anbefaler DI og DI ITEK, at artiklerne 35-36 ændres således, at der bliver tale om et kontaktpunkt hos virksomheden frem for en enkeltperson.
  Endelig er det centralt for virksomhederne at det præciseres, hvad der menes med en virksomhed, og herunder om kontaktpunktet kan etableres for hele virksomheden uanset, hvor mange lande virksomheden har en juridiske enhed med mere end 250 ansatte i.
- Artikel 35, stk. 5: DI og DI ITEK er af den opfattelse, af juridiske kompetencer ikke kan stå alene, men må suppleres med tekniske kompetencer. I stk. 5 bør det tilføjes, at den databeskyttelsesansvarlige foruden juridisk indsigt også bør have teknisk indsigt, og særligt bør der henvises til, at den databeskyttelsesansvarlige skal være i stand til at foretage vurderinger efter artikel 30, stk. 1 om databehandlingssikkerhed og dermed have kendskab til teknologiens aktuelle stade.
- Artikel 37, stk. 1: Blandt den DPO'ens forpligtelser bør der også være henvisning til at vurdere aktuelle sikkerhedsteknologier og –metoder. DI og DI

ITEK anbefaler derfor, at der til artikel 37, stk. 1 tilføjes et nyt litra i), som henviser til artikel 30 stk. 1 om databehandlingssikkerhed.

Kapitel V - XI

- Artikel 40ff: DI og DI ITEK noterer sig med glæde de forbedrede muligheder for at videreføre data til tredjelande. DI og DI ITEK må dog også notere sig, at forordningen desværre ikke forholder sig til at data i vidt omfang er globale, især i globale koncerner, som ikke nødvendigvis sondrer mellem dataenes oprindelsesland. En for rigid regulering kan medføre at europæiske virksomheder ikke kan få fuldt udbytte af omkostningsreducerende teknologier, herunder cloud.
- Artikel 42: DI og DI ITEK noterer sig med glæde de forbedrede muligheder for at videreføre data til tredjelande. Forholdet mellem Artikel 42 og Artikel 34 bør imidlertid præciseres jf. kommentarerne ved artikel 34.
- Artikel 73-76: Enhver fysisk eller juridisk person – herunder registrerede og "organer, organisationer eller sammenslutninger, der har til formål at beskytte registreredes rettigheder og interesser" – skal som angivet have ret til at klage til tilsynsmyndigheden eller en domstol. I det tilfælde, hvor en af de omtalte fysiske eller juridiske personer indklager til en flerhed af tilsynsmyndigheder eller domstole i de forskellige medlemslande, skal det på europæisk plan sikres, at én myndighed eller domstol behandler handler sagen. Årsagen er dels retssikkerheden for de europæiske borgere, som gerne skulle have samme afgørelse uanset land, og dels hensynet til administrative omkostninger hos controller eller processor. DI og DI ITEK anbefaler derfor, at det gøres muligt at skabe koordination mellem de europæiske domstole på dette område.
  Desuden anbefaler DI og DI ITEK, at forholdet mellem arbejdsgiver og arbejdstager undtages artikel 73 om mulighederne for offerløs klage. Sådanne forhold afklares i Danmark normalt mellem arbejdsmarkedets parter.
- Artikel 77: DI og DI ITEK foreslår som følge af kommentarer til Artikel 22 og 26 at det præciseres, at det er controllers ansvar og derfor controller, som kan være erstatningspligtig. Om controller inter partes kan "sende" erstatningspligten videre, må afhænge af kontrakten mellem controller og processor.
- Artikel 79: DI og DI ITEK er meget tilfreds med, at der sker en sidestilling af offentlige myndigheder og private virksomheder mht. administrative sanktioner. Det er vigtigt, at de administrative sanktioner også gælder EU's institutioner. Imidlertid forekommer bødestørrelserne helt ude af proportioner. Bøderne har en størrelse, hvor der er risiko for at lukke virksomheder. Bøderne har også en størrelse, som giver tilsynsmyndighederne incitament til en klapjagt på store virksomheder med mange penge uden at dette har nogen sammenhæng med risikoen for lovbrud. DI og DI ITEK anbefaler derfor, at maximum bødestørrelsen væsentligt reduceres, at bødestørrelserne ikke gøres indtægtsafhængige, samt at der tages særlige hensyn til uagtsomme overtrædelser samt overtrædelser af mere ordensmæssige forskrifter, hvor der ikke er sket nogen reel skade for registrerede. Der bør endvidere være

adgang til administrative påbud eller advarsler for mindre eller førstegangsforseelser. DI og DI ITEK foreslår, at der fastlægges en maksimal bødestørrelse af følgende størrelsesorden: et estimat af de økonomiske fordele hos controller eller processor (sparede omkostninger plus fortjeneste) ved at have forsyndet sig mod lovgivningen gange tre.

- Artikel 81: Behandling af helbredsoplysninger kan være nødvendigt for arbejdsgiver i vurdering af en nuværende eller potentielt kommende arbejdstager. DI og DI ITEK ønsker, at der eksplicit gøres opmærksom på, at arbejdsgiver skal kunne pålægge medarbejdere at fremskaffe lægeerklæringer ved sygemelding og evt. i andre sammenhænge, hvor en lægeerklæring kan være nødvendig for arbejdets udførelse.
- Artikel 82: Det er vigtigt, at arbejdsmarkedets kollektive overenskomster og aftaler fortsat kan regulere forhold på det danske arbejdsmarked. DI og DI ITEK ønsker, at der eksplicit henvises til aftaler mellem arbejdsmarkedets parter i stk. 1. Desuden ønsker DI og DI ITEK, at Kommissionens muligheder for at fastsætte delegerede retsakter på dette område fjernes og dermed at stk. 3 udgår. Det er vigtigt, at "Den Danske Model" ikke kan undermineres af Kommissionen.
- Artikel 90: Det er vigtigt, at loven efterlever dens formål – og det ved vi først, når loven har været i drift i nogle år. DI foreslår, at der laves en ny artikel 90, stk. 2, hvor det kræves, at de af kommissionen vedtagne delegerede retsakter evalueres hvert andet år og at denne evaluering forelægges Rådet, parlamentet og offentligheden, jf. stk. 1.

Bemærkninger til direktivet

DI og DI ITEK har ikke indgående studeret direktivet og har derfor ikke nogen detaljerede kommentarer på nuværende tidspunkt.

Imidlertid har vi noteret os bemærkningerne fra EDPS, som stiller spørgsmål til, hvorfor der er behov for et særligt direktiv for de retshåndhævende myndigheder. DI og DI ITEK anbefaler, at der lyttes til EDPS bemærkninger.

DI og DI ITEK står naturligvis til rådighed for en uddybelse af ovenstående kommentarer.

Med venlig hilsen

Henning Mortensen
Chefkonsulent
DI ITEK

MEDICO
INDUSTRIEN

Nivaagaard
Gl. Strandvej 16
DK-2990 Nivå

Tel. +45 4918 4700
Fax +45 4918 4707
medico@medicoindustrien.dk
www.medicoindustrien.dk

Justitsministeriet
Att. Christian Wiese Svanberg
Sagsnr. 2012-3756-0005
jm@jm.dk

29. juni 2012

Vedr. generel forordning om databeskyttelse

Ved mail af 11. maj 2012 har Justitsministeriet fremsendt forslag til generel forordning om databeskyttelse i høring i Medicoindustrien.

Helt overordnet er det Medicoindustriens synspunkt, at hensynet mellem beskyttelse af fysiske personers oplysninger skal balanceres op i mod medicobranchens behov for at forske og udvikle nye, innovative produkter til gavn for patientbehandlingen.

Det er på nuværende tidspunkt vanskeligt at få det fulde overblik over, præcis hvilke implikationer for branchen forordningen får, såfremt den gennemføres med sit nu foreliggende indhold, men Medicoindustrien har med tilfredshed noteret sig, at den endelige danske holdning til forslaget bl.a. vil afhænge af, om balancen mellem modsatrettede hensyn er fornuftig, f.eks. hensynet til forskning og udvikling og virksomhedernes rammevilkår. Også områder som telemedicin og elektroniske patientjournaler ville vi forvente bliver berørt af forordningen, og disse områder er meget afgørende for den fremtidige udvikling af sundhedsvæsenet hvor flere patienter 'udlægges' til eget hjem, snarere end at være indlagt på traditionel vis.

Medicoindustrien kan fuldt tilslutte sig, at der ved vurderingen af denne balance lægges stor vægt på hensynet til, at en vækstbranche som vores fortsat har mulighed for at forske og udvikle nye produkter, så Danmark kan bevare den styrkeposition vi har indenfor sundhedsindustrien generelt og specifikt indenfor området for medicinsk udstyr.

Venlig hilsen

Lene Laursen
Vicedirektør

Lægemiddel
Industri
Foreningen

Lersø Parkallé 101
2100 København Ø
Telefon 39 27 60 60
Telefax 39 27 60 70

info@lif.dk
www.lif.dk

Dato: 29-06-2012

Lifs høringssvar til Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) *(KOM(2012) 11 endelig)*

Lægemiddelindustriforeningen, Lif, hilser Kommissionens bestræbelser på at harmonisere databeskyttelseskravene yderligere i EU velkommen. De forskelligartede krav til beskyttelse af personoplysninger gør det vanskeligt for lægemiddelindustrien at udføre biomedicinsk forskning, som kan føre til opdagelsen af nye lægemidler, og det skaber særlige udfordringer for indsamling og rapportering af sikkerhedsdata vedrørende lægemidler.

Lif er meget tilfreds med forslagets grundlæggende anerkendelse af, at det af hensyn til offentlighedens interesse i at sikre fortsatte medicinske fremskridt og forskning er nødvendigt med særlige regler for indsamling og brug af personlige data til brug for medicinsk forskning (Artikel 83), og at offentlighedens interesse i medicinske fremskridt ligeledes retfærdiggør indsamlingen og brugen af data til formål inden for offentlig sundhed (Artikel 81, stk. 1). Begge aktiviteter finder allerede sted i dag under strengt kontrollerede og regulerede forhold, som er udformet til at beskytte patienters privatliv.

Lif mener, at der i forhold til det fremsatte forslag er behov for nogle mindre ændringer for at undgå utilsigtede og uønskede negative indvirkninger på den medicinske forskning.

- Særlige krav til nøglekodede data: Patienters identiteter skjules før kliniske forsøgsdata bliver rapporteret fra forsøgsstedet til lægemiddelvirksomhederne. Medmindre en person tager ekstraordinære midler i anvendelse, kan "nøglekodede data" kun blive re-identificeret via adgang til en nøgle, som opbevares sikkert på hvert forsøgssted. I forhold til forslagets artikler vedrørende dette, har Lif følgende bemærkninger:

  - Kodning af data bør tilføjes som en anerkendt måde, hvorved persondata kan sikres før, de overføres til et tredjeland (Artikel 42). En overførsel af nøglekodede data til brug for videnskabelig forskning bør ikke kræve yderligere godkendelse eller høring i tilfælde, hvor modtageren ikke har adgang til nøglen, og hvor kontraktlige eller juridiske restriktioner forbyder genidentifikation af de personer, dataene vedrører.

  - Forordningens krav om anmeldelse af brud på persondatasikkerheden bør ikke gælde nøglekodede data, forudsat at selve nøglekoden er intakt (Artikel 31). Nøglekodede data er ikke uden videre identificerbare, medmindre nøglen brydes samtidigt.

  - Videnskabelig forskning udført i overensstemmelse med Artikel 83 bør tilføjes til Artikel 6, stk. 4 som et juridisk og kompatibelt grundlag for at behandle personlige data yderligere. Denne æn-

dring er ganske vist i overensstemmelse med Artikel 6, stk. 1.b i Databeskyttelsesdirektivet af 1995, som foreskriver, at "Yderligere behandling af data til historiske, statistiske og videnskabelige formål ikke skal betragtes som inkompatible, forudsat at medlemsstaterne sørger for passende beskyttelse". Det afspejler også formålet beskrevet i Artikel 179, stk. 1 i Traktaten om EU's virke vedr. opnåelse af det europæiske forskningsrum.

- En gennemført konsekvensanalyse vedrørende databeskyttelse (Artikel 33) på specifikke data/databehandlinger bør også gælde andre persondatabehandlinger, der er af samme natur og som udgør de samme risici for privatlivet, som set i forbindelse med den første analyse. Et krav om at udføre flere og gentagne konsekvensanalyser af lignende databehandlingsaktiviteter vil tilføre en administrativ byrde uden at forøge databeskyttelsen yderligere.
  - En enkelt konsekvensanalyse bør være tilstrækkelig til, at identificere potentielle risici og strategier til reduktion af risici relateret til lignende brug af nøglekodede data til brug for videnskabelig forskning. Det samme gælder for indsamling og rapportering af oplysninger om lægemidlers bivirkninger.

- Den foreslåede definition af "genetiske data" er alt for bred og vil gøre nedarvede karaktertræk såsom øjen- og hårfarve til følsomme data, som kræver øget beskyttelse (Artikel 4, stk. 10).
  - En mere præcis definition baseret på eksisterende internationale standarder kunne være: "Oplysninger om arvelige karaktertræk eller ændring heraf, af en identificeret eller identificerbar person, opnået via nukleinsyre analyser."

- Processen vedrørende Kommissionens vedtagelse af delegerede retsakter bør kræve høring blandt relevante interessenter (Artikel 86 og andre).
  - For eksempel bør forskere høres i forbindelse med implementeringen af Artikel 17 (bevaring af persondata, som er nødvendige i forbindelse med offentlig sundhed og videnskabelig forskning) og Artikel 83, stk. 3 (begrænsninger i den registreredes ret til indsigt og adgang, hvor det er nødvendigt af hensyn til videnskabelige forskningsformål).

Med venlig hilsen

Henrik Vestergaard
Viceadministrerende direktør

Allan Skårup Kristensen
Chefkonsulent

Fra: Videnskabsetisk Komité [vek@rn.dk]
Sendt: 29. juni 2012 09:29
Til: Justitsministeriet
Emne: Vedr. Justitsministeriets j.nr. 2012-3756-0005

Til Justitsministeriet

Justitsministeriet har ved mail af 11. maj 2012 sendt Europa-Kommissionens forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) i høring til bl.a. Den Videnskabsetiske Komité for Region Nordjylland.

Komitéen takker ministeriet for denne mulighed, men har intet at bemærke til det fremsendte.

På komitéens vegne

Med venlig hilsen

Karina Østergaard Schøler
9635 1042
E-mail: k.oestergaard@rn.dk

REGION NORDJYLLAND
Patientdialog og
Sekretariatet for Den Videnskabsetiske Komité for Region Nordjylland
Niels Bohrs Vej 30
9220 Aalborg Ø
www.rn.dk

jm@jm.dk

Den 29. juni 2012

DOK. NR.:
FAID-6-8131
SAG. NR:
FAID-6-8019
Anders Feldt

Svar på høring om forordningsforslag om persondata – j.nr. 2012-3756-0005

Finanssektorens Arbejdsgiverforening (FA) har følgende bemærkninger til forordningsforlaget om databeskyttelse samt til Justitsministeriets grund- og nærhedsnotat om forslaget.

Som arbejdsgiverforening for den finansielle sektor er fokus for FA's høringssvar alene forslagets arbejds- og ansættelsesretlige konsekvenser.

Retsakt
Valget af en forordning som retsakt er ikke hensigtsmæssig set fra et arbejdsretligt perspektiv. I Danmark er løn- og ansættelsesforhold hovedsageligt reguleret af kollektive overenskomster, som er indgået af arbejdsmarkedets parter. Det følger af TEUF art. 153, at EU anderkender nationalstaternes kollektive arbejdsretlige systemer. Det fremgår derfor ligeledes af art. 153, at EU-retlig regulering af arbejdsmarkedsforhold sker ved udstedelse af direktiver med minimumsforskrifter under hensyn til de vilkår og tekniske bestemmelser, der gælder i hver af medlemsstaterne.

Det synes på det grundlag uforeneligt med TEUF art. 153, at regulere om forhold af betydning for ansættelsesforhold via en forordning. Den rette retsakt for sådanne reguleringer er direktivformen.

Det giver mulighed for tilpasning til de nationale arbejdsretlige systemer. Dette skal også ses i forhold til forordningsforslagets art. 82, hvorefter medlemsstaterne alene kan vedtage specifikke bestemmelser i forbindelse med ansættelsesforhold, hvis disse bestemmelser overholder forordningen. Med formuleringen af art. 82 efterlades der kun et minimalt spillerum for nationale tilpasninger om persondataoplysninger i ansættelsesforhold.

Forordningsforslaget giver endvidere anledning til følgende bemærkninger:

Samtykke – artikel 6, 7 og 9
Det fremgår af artikel 6 og 9, at det bl.a. er lovligt at behandle personoplysninger samt særlige personoplysninger, hvis der foreligger et samtykke.

Det fremgår imidlertid af artikel 7, stk. 4, at samtykke ikke udgør et retsgrundlag for behandling, hvis der er en klar skævhed mellem den registrerede og den registeransvarlige. Ifølge præamblen til forslaget er der tale om en klar skævhed, når den registrerede befinder sig i et afhængighedsforhold til den registeransvarlige, bl.a. når personoplysninger behandles af arbejdsgive-

ren som led i behandlingen af ansattes personoplysninger i et ansættelsesforhold.

Artikel 7, stk. 4 med bemærkninger i præamblen, vil derfor udhule enhver mulighed for i ansættelsesforhold at persondatabehandle på grundlag af et samtykke - hvilket er klart uacceptabelt. Efter FA's opfattelse er der ikke reel grund til at afskære brugen af samtykke i ansættelsesforhold, jf. at enhver behandling af personoplysninger er omfattet af de generelle principper for behandling i art. 5, hvilket vil sige, at oplysningerne bl.a. skal behandles loyalt og legitimt.

Hertil kommer, at der består et reelt behov for at kunne behandle personoplysninger og særlige oplysninger som led i ansættelsesforholdet. F.eks. kan det være hensigtsmæssigt, at arbejdsgiveren kan behandle helbredsmæssige oplysninger ved medarbejderens sygefravær eller ved ansættelse af medarbejdere omfattet af overenskomsternes sociale kapitler samt for medarbejdere, der er visiteret til flexjob.

Det er herunder meget usikkert, om en arbejdsgiver overhovedet må behandle helbredsoplysninger, når art. 7, 9 og 81 sammenholdes. Hvis arbejdsgiver ikke kan behandle helbredsoplysninger, vil det vanskeliggøre indsatsen for at bevare medarbejderens tilknytning til virksomheden og arbejdsmarkedet.

Endvidere vil det være yderst indgribende, hvis arbejdsgiverne afskæres muligheden for at indhente og behandle straffeattester i ansættelsesforhold, som arbejdsgiver bl.a. i den finansielle sektor, næsten har et undtagelsesfrit behov for at kunne gøre. Ved samtykke er indhentelsen af straffeattesten fortsat underlagt kravene i art.5

Samtykke bør derfor fortsat være lovlig behandlingsgrund i ansættelsesforhold. Både når det gælder personoplysninger i art. 6 og særlige personoplysninger i art. 9. Ved at benytte samtykke som behandlingsgrundlag i ansættelsesforhold, sikrer man et klart og tydeligt behandlingsgrundlag for arbejdsgiver og medarbejder.

Opretholdelse af arbejdsretlige forpligtelser - artikel 9, stk.1, litra b
Efter art. 8, stk. 2 i det gældende direktiv 95/46/EF kan særlige personoplysninger behandles, hvis behandlingen er nødvendig for overholdelsen af den registeransvarliges arbejdsretlige forpligtelser og specifikke rettigheder. Udtrykket arbejdsretlige forpligtelser forstås i Danmark bredt og gælder alle former for forpligtelser og rettigheder, der bygger på et arbejdsretligt grundlag. Dette gælder, uanset om grundlaget er lovgivning eller kollektiv aftale. Det bør derfor tilføjes i forordningsforslagets art. 9, stk. 2 litra b, at undtagelsen også gælder, hvis den er hjemlet i kollektive aftaler, som fastsætter de fornødne garantier.

Udpegning af databeskyttelsesansvarlig – artikel 36
Det fremgår af art 35, pkt. 7, at den databeskyttelsesansvarlige kun kan afskediges, hvis vedkommende ikke længere opfylder betingelserne for at varetage hvervet.

Det er usikkert, hvordan denne bestemmelse skal fortolkes, men umiddelbart fremstår den som meget vidtgående, da den synes at være knyttet op på forordningens betingelser. Rent ansættelsesretligt er dette hverken rimeligt eller betryggende – og udgør et indgreb i gældende national lovgivning og indgåede overenskomster.

Arbejdsgiver bør kunne afskedige den dataansvarlige i de situationer, hvor det må vurderes som rimeligt eller nødvendigt ud fra de faktiske omstændigheder. Som alternativ kunne foreslås en formulering i lighed med det man kender fra ligebehandlingsloven og forskelsbehandlingsloven: "Den dataansvarlige må ikke afskediges på grund af varetagelsen af hvervet som dataansvarlig, hvis vedkommende fortsat opfylder betingelserne for at varetage hvervet, og hvervet udføres forsvarligt og i overensstemmelse med forordningens bestemmelser."

Administrative sanktioner - artikel 79.
Forslaget om at en virksomhed kan idømmes bøder på op til 2 pct. af virksomhedens globale omsætning er uproportionalt i forhold til overtrædelsernes karakter. Dette skal sammenholdes med, at art. 79, stk. 4, 5 og 6 umiddelbart må forstås således, at tilsynsmyndigheden *skal* pålægge bøder i de pågældende tilfælde. Der bør være større rum for tilsynsmyndigheden til at give advarsler efter art. 79 stk. 3 og endvidere må bødestørrelserne stå i forhold til generel national praksis. De vejledende bødestørrelser bør derfor udgå af forordningen, så bøderne forholdsmæssigt tilpasses de enkelte nationalstaters øvrige lovgivning.

Behandling af personoplysninger om helbredsforhold - artikel 81
I Danmark er løn og ansættelsesvilkår hovedsageligt reguleret i kollektive overenskomster. Det bør derfor tilføjes i art. 81, at helbredsoplysninger også kan behandles på grundlag af kollektive overenskomster, da især stk. 1, litra c, kan omfatte områder, der i Danmark er reguleret i de kollektive aftaler.

Behandling i forbindelse med ansættelsesforhold - artikel 82
Under art. 82 bør det tilføjes, at også arbejdsmarkedets parter kan vedtage specifikke bestemmelser, der regulerer behandlingen af arbejdstageres personoplysninger. Det fremgår af præamblens nr. 124, at medlemsstaterne ved lov kan indføre specifikke regler for behandling af personoplysninger ved ansættelsesforhold.

Da arbejdsretlige forhold i Danmark hovedsageligt er reguleret i kollektive overenskomster og ikke i lovgivningen, er det afgørende, at også arbejdsmarkedets parter kan vedtage bestemmelser, der regulerer behandlingen af arbejdstagers personoplysninger. Alt andet vil være i strid med den danske model. Det er derfor væsentligt, at forordningen kan imødekomme kollektive aftaler som indgås af arbejdsmarkedets parter. Endvidere skal gældende kollektive aftaler kunne videreføres.

Delegerede retsakter – artikel 86
Antallet af delegerede retsakter er meget omfattende, og de må forventes at få stor betydning for den endelige forståelse af det samlede regelsæt. I overensstemmelse med bemærkning 129 i præamblen, er det afgørende, at Kommissionen gennemfører relevante høringer, når beføjelsen til at udstede delegerede retsakter benyttes.

Med venlig hilsen

Anders Feldt