Rådet for Digital Sikkerhed

18. august 2017

Rådet for Digital Sikkerheds høringssvar til forslag til databeskyttelsesloven

Rådet for Digital Sikkerhed, RfDS, skal hermed takke for muligheden for at afgive høringssvar til "udkast til forslag til databeskyttelsesloven", DBL. RfDS benytter sig af lejligheden til samtidig at komme med enkelte bemærkninger til betænkning 1565, da betænkningen udgør et væsentligt fortolkningsbidrag til at forstå formuleringen af databeskyttelsesloven.

1. Overordnede bemærkninger

Ros til JM for et grundigt arbejde

RfDS vil indledningsvis takke Justitsministeriet, JM, for betænkning 1565. Betænkningen er et stort og grundigt arbejde, som er lavet på relativt kort tid henset til omfanget. Betænkningens format er, med dens opsummering af gældende ret, sammenligning med forordningens regler og mange steder gennemgang af relateret praksis og retspraksis, et værk som er yderst anvendeligt til en forståelse af persondataretten i en dansk kontekst. Betænkningen kan anvendes som opslagsværk for de fagpersoner, som skal beskæftige med området mange år fremover.

RfDS siger hermed mange tak til JM for en grundig og nyttig betænkning.

Glæde over de kommende vejledninger

RfDS noterer sig samtidig, at JM er klar over, at betænkningen ikke kan stå alene. På trods af dens kvalitet vil den næppe få en bred læserskare henset til dens omfang. Derfor noterer RfDS sig med glæde, at der også er planlagt en serie af vejledninger, som kortfattet og populært skal opsummere en række af betænkningen og databeskyttelseslovens regler, så de bliver tilgængelige for borgere, virksomheder og organisationer.

RfDS skal hermed udtrykke tilfredshed med, at der udarbejdes en serie kortfattede vejledninger om DBL og den praksis, den medfører.

Ændringer i gældende ret skal understreges og fortolkes harmoniseret

RfDS noterer sig, at JM gennem arbejdet med såvel betænkningen som databeskyttelsesloven har analyseret persondataforordningen således, at så store dele af gældende dansk ret kunne opretholdes som overhovedet muligt. RfDS er ikke begejstret for denne tilgang, da vi gerne så, at reglerne på det persondataretlige område overordnet bliver så harmoniserede som muligt indenfor EU. Det synes således at have været JMs ønske at nå den konklusion, at der ikke er tale om en ændring af gældende ret på trods af, at der i en række tilfælde er tale om, at der i lovgivningen inkluderes helt nye begreber. I de detaljerede bemærkninger nedenfor vil RfDS påpege et par eksempler på dette, f.eks. mht. konsekvensanalyser og databeskyttelse gennem design. I nær tilknytning hertil er det RfDS håb, at de kommende vejledninger tæt vil reflektere de vejledninger, der kommer fra artikel 29-gruppen, således at der ikke er risiko for, at det fremstår som om, at der er forskellig fortolkningspraksis mellem JM og artikel 29-gruppen.

RfDS håber, at man i det fremadrettede arbejde i høj grad vil skele til andre europæiske vejledninger på det persondataretlige område – herunder særligt fra artikel 29-gruppen – således at reglerne bliver så harmoniserede som muligt indenfor EU.

Der ligger et stort arbejde foran danske virksomheder og organisationer

RfDS noterer sig ligeledes, at JM i såvel betænkningen som i den kommunikation der har været om forordningen, betænkningen og databeskyttelsesloven understreger, at forordningen alene giver anledning til mindre justeringer af gældende ret og at det derfor for virksomheder og organisationer, som efterlever de eksisterende regler, ikke er en stor opgave at efterleve de nye regler. JM når frem til denne konklusion ved snævert at sammenligne de eksisterende regler med de fremtidige regler. RfDS kan ikke genkende dette billede. For det første er der i lovgivningen en introduktion af en række nye begreber og tilknyttede bestemmelser, som skal efterleves, jf. ovenfor. For det andet er der givetvis ganske mange virksomheder og organisationer, som ikke efterlever de eksisterende regler. Dette store flertal af virksomheder og organisationer vil opleve nødvendigheden af at efterleve gamle såvel som nye regler som en ganske stor arbejdsopgave. Når man sammenligner virkeligheden med de kommende regler, skal der gøres en betydelig indsats for at efterleve reglerne. For de projektledere, DPO'er, CPO'er m.v. som sidder med opgaverne bliver det ikke lettere at få ressourcer til arbejdet, når JM i sin kommunikation underdriver arbejdets omfang. For det tredje udestår der fortsat en lang række spørgsmål, når juraen skal anvendes på konkrete omstændigheder i den virkelige verden - ikke mindst fordi denne lovgivning i meget høj grad lægger op til et konkret skøn af forskellige forhold og tillige på mange områder er baseret på en retspraksis, som man ikke kan læse sig til direkte i lovgivningen. Det er skøn, som det er vanskeligt at foretage for virksomheder og organisationer, som ikke har en ekspert tilknyttet og som ikke har et budgetmæssigt rum til at få det.

RfDS skal opfordre til, at JM i sin kommunikation ikke nedtoner forbedringerne i de nye regler eller tager let på de udfordringer, som virksomheder og organisationer står overfor, når de skal til at efterleve de nye regler.

Styrkelse af Datatilsynet

RfDS noterer sig yderligere, at JM i betænkning 1565 i afsnit 7.5.4 ikke i fornødent omfang understreger det store merarbejde, som forordningen vil betyde for Datatilsynet. Hermed er der en risiko for, at der ikke fra politisk side er den fornødne opmærksom på at styrke Datatilsynet tilstrækkeligt. Når man sammenligner de opgaver, der pålægges Datatilsynet i direktiv 95/46/EF, artikel 28 med beskrivelsen i forordningens artikel 57 kan man konstatere, at der er tale om et meget betydeligt øget omfang af arbejdsopgaver. Der er i praksis kun få arbejdsopgaver der ændres, og endnu færre der falder bort. Det ligger RfDS meget på sinde, at især artikel 57, stk. 1, litra b, d og i, som omhandler den viden om reglerne, som Tilsynet pålægges at bibringe omverdenen, bliver på et tilfredsstillende niveau. Desuden er det vigtigt, at der er fokus på den EU-harmonisering, som forordningen trods alt stadig giver mulighed for, og som er defineret som Tilsynets arbejdsopgaver og især adresseres i artikel 57, litra g, h og t. RfDS mener, at vi har brug for et Datatilsyn, som ikke kun er Tilsyn, men også i høj grad kan informere konkret om reglernes anvendelse, når der er brug for det. Et tilsyn som kan agere proaktivt, har ressourcer til at tage sager op af egen drift, har moderne kommunikationsfaciliteter, er involveret i den offentlige debat, tager stilling til konkret anvendelse af nyere teknologier, har en åbningstid der svarer til omverdenen, fungerer som et nationalt kompetencecenter for persondatabeskyttelse (gerne med tilknytning til såvel den juridiske som den tekniske forskningsverden) og som tilvejebringer vejledninger og redskaber til at understøtte offentlige og private organisationers implementering af forordningens regler.

RfDS vil derfor med dette høringssvar appellere til en markant styrkelse af Datatilsynet.

Udnyttelse af nationale særregler

Rådet noterer sig, at JM generelt har udnyttet mange af forordningens muligheder for at fastsætte national lovgivning. Rådet skal bemærke, at når disse muligheder udnyttes, så undermineres et af hovedformålene med forordningen; nemlig at skabe harmonisering i EU. Borgernes data vil blive behandlet forskelligt i de forskellige EU-lande. Virksomhederne i deres roller som dataansvarlige og databehandlere får øgede omkostninger, når de, for så vidt angår de områder hvor der udnyttes muligheder for at fastsætte national lovgivning, skal tilpasse deres it-systemer og procedurer til 28 forskellige nationale regelsæt. De nationale særregler vil være en hæmsko specielt for SMV'erne i forhold til at få adgang til det indre marked.

RfDS skal henstille til, at der fra politisk side tages hensyn til det indre markeds målsætninger om fri bevægelighed således at der kun anvendes national lovgivning, hvor det skønnes absolut nødvendigt.

2. Detaljerede bemærkninger til DBL

Krigsreglen

RfDS har noteret sig, at der er lagt op til en ændring af krigsreglen fra PDL § 41, stk. 4. Ændringen jf. DBL § 3, stk. 9 betyder, at man går fra at kunne bortskaffe personoplysninger i tilfælde af krig til at vurdere om personoplysninger i nærmere bestemte IT-systemer, må placeres i udlandet. Det bagvedliggende hensyn præciseres samtidig p. 259 til ikke at være IT-sikkerhed, men alene at være statens sikkerhed. På den måde må det forventes, at der bliver tale om en klart afgrænset og gennemsigtig liste af konkrete systemer, som ikke må placeres udenfor landets grænser. RfDS er meget tilfredse med denne modernisering og præcisering af krigsreglen, som implicit anerkender, at hvis IT-sikkerheden er på plads, så betyder det ikke noget, hvor i EU personoplysningerne er placeret.

RfDS er tilfreds med ændringen af krigsreglen men skal opfordre til, at der anlægges snævre betragtninger baseret på risikovurderinger af, hvilke IT-systemer, som kan omfattes af hensynet til statens sikkerhed.

Offentlige myndigheder kan viderebehandle til andre formål med undtagelser for oplysningspligten

RfDS er skeptiske overfor, at offentlige myndigheder jf. DBL § 5, stk. 3 kan få fastsat regler, der sikrer viderebehandling af personoplysninger til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed. RfDS finder for det første, at bestemmelsen er meget bred. Når først en offentlig myndighed er kommet i besiddelse af en personoplysning, kan den principielt set ende hvor som helst og anvendes til et hvilket som helst formål (selvfølgelig forudsat at der er en regel). Når denne bestemmelse så ses i sammenhæng med DBL § 23 og § 22, stk. 2 og 3 om undtagelserne i oplysningspligten og indsigtsretten, som betyder, at det bliver grænsende til umuligt for de registrerede at benytte rettighederne i artikel 16, 17, 18 og 21, betyder det, at DBL medvirker til at sikre en fuldstændig uigennemsigtighed for borgerne om, til hvilke formål og af hvilke myndigheder deres personoplysninger behandles. Tilsvarende gælder for behandling i videnskabeligt øjemed, jf. DBL § 22, stk. 5.

Det klæder ikke et demokratisk samfund at have sådanne regler. Det bør reducere tilliden til den offentlige sektors behandling af personoplysninger og formodentlig også til den offentlige sektors digitalisering.

Argumenterne for at den offentlige sektor skal have disse regler anføres bl.a. effektivitet (p. 168) og byrder (p.210). Der synes ikke at være tilsvarende betragtninger om, at der er byrdefuldt for de private virksomheder, som der ikke er tilsvarende undtagelser for, at efterleve reglerne. Der findes således en asymmetri i reglerne mellem den offentlige og private sektor.

Endelig finder RfDS, at man i hvert fald kan diskutere, om den undtagelsesbestemmelse, der er indsat i forordningens artikel 23, stk. 1, litra e om medlemsstaternes "væsentlige økonomiske eller finansielle interesser", og som JM anvender som retligt grundlag for undtagelserne, er tiltænkt denne anvendelse. Interesserne uddybes i litra e med "herunder valuta-, budget- og skatteanliggender". Man kan diskutere, om medlemsstaterne ikke alene bør anvende undtagelsesbestemmelsen snævert, når der er større forhold på spil, som f.eks. en væsentlig påvirkning af BNP, end at JM ønsker at købe billigere it-systemer og ønsker en billigere offentlig forvaltning. Hertil kommer at man kan diskutere om begrænsningen "respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i det demokratisk samfund", jf. artikel 23 stk. 1 og JMs egen formulering i § 22, stk. 2 om, at undtagelser kun bør anvendes, hvis der er "afgørende hensyn til offentlige interesser".

At sætte et de fundamentale principper fra forordningens artikel 5 ud af kraft samtidig med at man tilsidesætter nogle af de registreredes rettigheder i artikel 14 og 15, der gør det grænsende til umuligt for de registrerede at udnytte deres rettigheder fra artiklerne 16, 17, 18 og 21 og samtidig anvende en undtagelsesbestemmelse, som man i hvert fald kan diskutere om den ikke er tiltænkt vigtigere formål end de skitserede, synes stærkt betænkeligt.

JM anfører flere steder, at de nye regler ikke fører til en ændring af praksis, men tværtimod er fastsat for at opretholde eksisterende retspraksis, f.eks. p. 150. Uanset om der sker en ændring af praksis eller ej, synes det betænkeligt at have en praksis som skitseret ovenfor. Forordningen kunne anvendes som en anledning til at rette op på det, og give de registrerede en bedre beskyttelse.

RfDS skal opfordre til, at bestemmelsen i §5 stk. 3 fjernes således at alle myndigheder skal anvende §5, stk. 2 ved vurdering af, om to formål er forenelige. Desuden skal RfDS opfordre til, at bestemmelse i § 23 og § 22, stk. 2 anvendes langt mere snævert, end der er lagt op til, således at det kun er helt undtagelsesvist, at der er undtagelse for oplysningen om behandling. For så vidt angår DBL § 22, stk. 3 tager RfDS det til efterretning, at reglerne om indsigt efter DBL bringes i overensstemmelse med reglerne i forvaltningsloven.

De arbejdsretlige regler

DBL indeholder flere forskellige steder regler, som er af betydning for arbejdsretten, f.eks. DBL § 7, stk. 2 om følsomme oplysninger, § 8, stk. 3 og 4 om straffeoplysninger, herunder straffeattest og § 12 om generel behandling af personoplysninger på arbejdsmarkedet i medfør af lov og overenskomster. Særligt på det arbejdsretlige område fastslås det, at den offentlige forvaltning kan behandle oplysninger med interesseafvejning, selv dette i øvrigt generelt er udelukket den offentlige forvaltning. Det fastslås også, så der ikke er tvivl, at samtykke kan bruges som retligt grundlag for behandling af personoplysninger. RfDS

tager disse fortolkningsbidrag til efterretning, og vil gerne udtrykke tilfredshed med, at DBL sikrer, at der ikke skabes usikkerhed om reglernes anvendelsesområde på arbejdsmarkedet.

I det omfang en personoplysning via praksis har været klassificeret som en dansk PDL §8 oplysning om strafbare forhold, væsentlige sociale problemer og andre rent private forhold skal oplysningen reklassificeres som enten en almindelig eller en følsom oplysning, da de rent private oplysninger bortfalder med forordningen. Af artikel 10 om behandling af oplysninger om strafbare forhold fremgår det, at behandlingen kan foretages på baggrund af artikel 6 stk. 1, hvorfor oplysninger om strafbare forhold må anses for at være en art almindelig oplysning. Dette konkluderes også meget hurtigt i lovforslaget p. 174 og p. 187. Det er centralt at fastslå, at man ikke derfor kan konkludere, at alle PDL § 8 oplysninger automatisk bliver almindelige oplysninger under forordningen. I betænkningen findes i relation til artikel 88 en glimrende beskrivelse af det arbejdsretlige område herunder en beskrivelse af, hvilken klassifikation der gennem praksis er fastlagt. Det ville have været nyttigt, dersom JM i betænkningen havde taget stilling til en reklassifikation af de arbejdsretlige § 8 -oplysninger om rent private forhold. Personlighedstest, som hidtil har været en oplysning om rent private forhold kan f.eks. næppe passes ind i som en følsom oplysning efter artikel 7 og må derfor antages at være en almindelig oplysning efter artikel 6, hvorimod alkoholtest i form af blodprøver, som også hidtil har været en §8 oplysning om rent private forhold, formodentlig godt fremadrettet kan antages at være en helbredsoplysning og dermed en følsom oplysning efter artikel 9.

Da det arbejdsretlige område er af betydning for alle arbejdsgivere og lønmodtagere, skal RfDS hermed opfordre til, at der laves en særskilt vejledning eller udtalelse evt. fra Datatilsynet om reklassifikation af PDL § 8 oplysninger.

Sanktioner

RfDS har noteret sig, at der med § 42 er lagt op til, at Datatilsynet kan udstede bødeforlæg som nærmere omtalt p. 238 og p. 246. Såfremt bødeforlægget ikke accepteres, skal Datatilsynet foretage politianmeldelse med bl.a. indstilling om bødens størrelse. Desuden skal Datatilsynet jf. bemærkningerne p. 247 høres herunder om bødens størrelse førend der træffes afgørelse om tiltale spørgsmål.

RfDS vil gerne tilkendegive fuld støtte til at tildele Datatilsynet kompetencer, som angivet ovenfor, idet det på pragmatisk vis løser udfordringen med at udstede administrative bøder henset til begrænsningerne i Grundloven.

Videre noterer RfDS sig, at JM lægger op til at overtrædelsen af artikel 10 om oplysninger om strafbare forhold også skal strafsanktioneres i dansk ret. Det synes ganske rimeligt at strafsanktionere denne overtrædelse, ligesom det gør sig gældende for de øvrige almindelige og for de følsomme oplysninger.

RfDS kan derfor bakke op om, at der sanktioneres ved overtrædelse af artikel 10.

Endelig noterer RfDS sig, at der i JM udkast til DBL, jf. § 41, stk. 5 ikke er taget stilling til om offentlige myndigheder kan sanktioneres. RfDS finder, at det er rimeligt, at der introduceres bøder til den offentlige sektor. For det første har det en betydeligt større afskrækkende effekt at der kan trækkes penge ud af et budget til bøder end at der kan komme et brev fra Datatilsynet, hvori der udtales kritik. Bøder er med andre ord et meget stærkt incitament til at overholde loven. For det andet et det vigtigt for retfærdighedsopfattelsen i samfundet at der er lighed for loven. Den samme overtrædelse skal straffes ens

uanset om man er offentlig eller privat. For det tredje er det vigtigt, at der sker harmonisering i Europa. Danmark bør ikke være et discount land når det kommer til at straffe overtrædelser i den offentlige sektor. Når borgerne desuden skal være mobile jf. det indre marked, vil det forekomme besynderligt, hvis de lande de agerer i straffer de offentlige myndigheder forskelligt.

De fleste af argumenterne imod bøder til den offentlige sektor synes at kunne afvises. En offentlig myndighed, som får en bøde kan ikke reducere sine serviceforpligtelser, som typisk er lovbestemte – f.eks. plejehjem og børnehaver. Pengene skal hentes et andet sted – f.eks. på anlægsinvesteringer eller fra reserver. Et andet argument mod bøderne er at der sædvanligvis ikke udstedes bøder til det offentlige under henvisning til straffelovens § 27, stk. 2. Der findes dog adskillige eksempler på at den offentlige sektor alligevel kan modtage bøder – f.eks. på i forhold til arbejdsmiljølovgivningen, fødevarelovgivningen eller udbudsloven.

RfDS finder, at der skal ske en ligestilling mellem den offentlige og den private sektor, således at begge sektorer kan idømmes de samme bøder for de samme overtrædelser.

Brede rammer for regeringen til at lave nationale bestemmelser

RfDS noterer sig, at der med § 44 indføres ganske vide bestemmelser for både Justitsministeren og for andre ministre indenfor deres ressort at fastlægge særregler uden at disse skal forelægges Folketinget – ikke mindst jf. uddybningen pp. 321-322.

RfDS finder, at denne problemstilling er tæt relateret til den problemstilling, som fremgik af Kommissionens oprindelige udkast til forordning fra januar 2012, hvoraf det fremgik, at Kommissionen på en meget lang række områder kunne udstede delegerede retsakter, med det formål at sikre en stærk harmonisering af reglerne. Kommissionens ret til at fastsætte delegerende retsakter er under forhandlingerne om forordningen blevet væsentligt reduceret, bl.a. fordi man var bange for at det ville skabe uforudsigelighed i regeldannelsen, hvis man administrativt kunne fastsætte sådanne regler. Hvis alle medlemsstaterne benytter sig af tilsvarende muligheder for løbende at fastsætte regler efter behov får man den samme forudsigelighed bare på nationalt. Det er en endnu værre situation, fordi vi så med sikkerhed får 28 forskellige implementeringer og dermed en lige så fragmenteret lovgivning, som under det eksisterende direktiv 95/46/EF.

Rådet anser tiltag som § 44 for at kunne medvirke til en begrænsning af harmoniseringen af reglerne på det persondataretlige område og opfordrer til, at § 44 kan fjernes eller indskrænkes mest muligt.

3. Detaljerede bemærkninger til betænkningen

RfDS har foruden bemærkninger, der knytter sig til DBL, også en række andre bemærkninger vedrørende persondataretlige forhold. Da disse bemærkninger formodentlig ikke vil indgå i JMs overvejelser i relation til høring af loven, vil RfDS formodentlig rette en selvstændig og direkte henvendelse til Justitsministeren desangående.

Backup

RfDS anser det for en væsentlig praktisk udfordring, hvordan man i fremtiden skal indrette sine backupløsninger. Backup er en kopi af såvel data som it-systemer, der gemmes separeret fra de oprindelige data og it-systemer med henblik på at kunne bringes i anvendelse, hvis de oprindelige data eller it-systemer rammes af fejl, ondsindet kode som f.eks. ransomware eller tyveri i form af hacking og dermed ikke længere er tilgængelige eller har fået krænket fortrolighed eller integritet.

I sikkerhedsstandarden ISO/IEC 27002:2013 kontrol 12.3 fremgår det, at: "Der bør tages backupkopier af informationer, software og systembilleder, og disse bør testes regelmæssigt i overensstemmelse med den aftalte backuppolitik". Standarden skal efterleves af statslige myndigheder. I den seneste digitaliseringsstrategi er der en hensigt om at regioner og kommuner efterlever den. Desuden efterlever mange private virksomheder standarden. Backup er med andre ord et teknisk sikkerhedstiltag, som i mange år har været en følge af god sikkerhedsskik, sikkerhedsstandarder, og anbefalet af offentlige myndigheder.

Det følger af standarden m.v., at der etableres en backuppolitik, som skal testes. En række backupløsninger er baseret på princippet om, at de ikke kan ændres, fordi det i sig selv er en sikkerhedstrussel, hvis backupdatas eller -it-systemers integritet er udfordret: Hvis f.eks. en online harddisk backup kan ændres, kan den inficeres med ransomware samtidig med at produktionsdata og produktionssystemer inficeres, og så har organisationen ikke længere en backup.

Direktiv 95/46/EF, artikel 17, stk. 1, Lov om behandling af personoplysninger, § 41, stk. 3 og forordningens artikel 32, stk. 1 lægger op til, at dataansvarlige og databehandleren skal gennemføre "evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse" (litra c), hvilket i en række tilfælde kun kan ske ved at genindlæse en backup. Der er i medfør af lovgivningen med andre ord en pligt til at tage backup, da det er den eneste måde, man i forhold til en række konkrete sikkerhedsbrud vil kunne genoprette oplysningerne.

Den registreredes ret til sletning er fastslået i direktiv 95/46/EF, artikel 12, litra b, Lov om behandling af personoplysninger §37 og i forordningens artikel 17, hvor det i stk. 1 hedder: "Den registrerede har ret til at få personoplysninger om sig selv slettet af den dataansvarlige uden unødig forsinkelse, og den dataansvarlige har pligt til at slette personoplysninger uden unødig forsinkelse" under forudsætning af at et af flere forhold gør sig gældende. Retsstillingen mht. indsigt og sletning er med forordningen ikke ændret væsentligt.

RfDS finder, at der er en konflikt mellem på den ene side at tage backup og på den anden side at efterkomme en anmodning om sletning eller berigtigelse. Teknisk er det i en række sammenhænge umuligt at berigtige eller slette personoplysninger fra backup. Uanset at retsstillingen er uændret med forordningen, er det en udfordring, som aldrig er blevet løst. RfDS skal anmode om, at JM evt. med hjælp fra Digitaliseringsstyrelsen og Datatilsynet, supplerer sin liste over planlagte vejledninger med en vejledning om, hvordan man teknisk skal kunne efterleve dette krav.

Konsekvensanalyser

I betænkningen har JM gennemgået reglerne for, hvornår der skal udarbejdes konsekvensanalyser pp. 522-537. Reglerne er gennemgået helt således som de præsenteres i forordningen: der skal lægges vægt på om behandlingen udgør en høj risiko for de registrerede og de tre eksempler, der gives i forordningens artikel

35, stk. 3, på hvornår der skal gennemføres konsekvensanalyser, er gengivet. JM fastslår herefter, at der er tale om en udvidelse af gældende ret, og drager samtidig den konklusion baseret på eksemplerne og flere præambelbetragtninger, at "området for, hvornår en konsekvensanalyse er påkrævet er snævert. Dataansvarlige må således i de fleste tilfælde antages ikke at skulle udarbejde en konsekvensanalyse", p. 534.

JMs gennemgang af konsekvensanalyserne synes præget af at understrege at der for langt de fleste dataansvarlige ikke sker noget nyt med forordningen. RfDS finder, at JM's gennemgang på den ene side er ordentlig og saglig men på den anden side er overdrevet forsigtig i forhold til at stille nye krav. F.eks. har artikel 29-gruppen i wp 248, pp. 7-9 opstillet 10 kriterier for, hvornår virksomheder og organisationer skal overveje at gennemføre konsekvensanalyser. Disse kriterier synes at udvide anvendelsen af konsekvensanalyser ud over hvad der redegøres for af JM. Kriterierne blev vedtaget i april og har i øvrigt været kendt i udkast længe, altså et godt stykke tid inden udgivelsen af betænkningen.

RfDS vil gerne påpege, at området for anvendelsen af konsekvensanalyser synes lidt bredere, end det umiddelbart fremgår af betænkningen. RfDS vil samtidig påpege, at det er vigtigt, at rådgivningen fra offentlige myndigheder mht. de persondataretlige regler ikke er for forsigtig. Det er dyrt at skulle lave løsninger om, hvis kravene bliver fortolket mere skærpet end først antaget, end det er at lave løsningerne mere sikre fra starten.

Databeskyttelse gennem Design

Databeskyttelse gennem design, DPbD, kendes ikke som juridisk begreb fra hverken persondatadirektivet eller persondataloven. Det er et nyt begreb, som introduceres i persondataforordningens artikel 25. I Betænkningen konkluderer Justitsministeriet imidlertid, at området er "dækket af flere bestemmelser i gældende ret", p.410, og at "Databeskyttelsesforordningens artikel 25 etablerer ikke i sig selv nye krav til den dataansvarlige", p. 422. RfDS er uenig i den udlægning af forordningen. RfDS finder, at JM også på dette område er for forsigtige med at bruge forordningen til at tolke et nyt indhold ind i persondataretten.

JM fastslår herefter, at artikel 25 stiller krav til, at der skal gennemføres passende tekniske og organisatoriske foranstaltninger både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen. Det fastslås af JM, at det er nyt, at foranstaltningerne skal fastlægges på tidspunktet for fastlæggelse af midlerne. RfDS er enig i denne betragtning.

RfDS mener, at artikel 25 stiller nye krav til de dataansvarlige. Når JM når frem til deres konklusion skyldes det formodentlig, at JM finder, at der er overensstemmelse mellem de passende tekniske og organisatoriske foranstaltninger, der stilles efter artikel 25 og artikel 32. RfDS finder derimod, at der er tale om to typer af foranstaltninger, hvorefter den ene type kan siges at være designkrav, mens den anden type kan siges at være sikkerhedskrav. På visse punkter er der et overlap mellem de to typer af foranstaltninger forstået således, at en given foranstaltning godt kan være både designmæssig og sikkerhedsmæssigt begrundet, f.eks. pseudonymisering. RfDS mener derfor, at JM overser et selvstændigt materielt indhold i artikel 25.

I artikel 32 stilles der krav om foranstaltninger, der skal passe til de risici den teknologiske løsning indebærer. Der nævnes eksempler på teknologier i form af pseudonymisering og kryptering, der nævnes målsætninger som tilgængelighed, fortrolighed, integritet og robusthed og der nævnes organisatoriske tiltag som tests. Listen kan siges at være uddybet i sikkerhedsbekendtgørelsen, hvor der nævnes konkrete tiltag som logning, adgangskontrol og fysisk sikkerhed. Sikkerhedsbekendtgørelsen falder imidlertid bort med

forordningen og afløses af en konkret risikovurdering af hvilke foranstaltninger, der er behov for. I artikel 32 gives der altså eksempler på hvad sikkerhed er, men der stilles ikke eksplicitte krav til hvilke foranstaltninger, der skal iværksættes. Den dataansvarlige skal selv vurdere hvilket materielt indhold, der ligger i bestemmelsen ud fra sine konkrete behandlinger, risici, m.v.

Tilsvarende i artikel 25, hvor der som eksempler på teknologier nævnes pseudonymisering og som målsætninger nævnes dataminimering, andre databeskyttelsesprincipper og tilgængelighed. Artikel 25 giver altså også eksempler på, hvad der skal forstås ved design, men der stilles ikke eksplicitte krav til hvilke foranstaltninger, der skal iværksættes. RfDS mener, at også her skal den dataansvarlige selv vurdere hvilket materielt indhold, der ligger i bestemmelsen ud fra sine konkrete behandlinger, risici, m.v.

Til støtte for dette synspunkt kan det konstateres, at begrebet passende tekniske og organisatoriske foranstaltninger anvendes flere steder i forordningen. Det er imidlertid ikke givet, at betydningen af ordvalget er den samme i alle situationer. F.eks. i artikel 28, stk. 3 litra e er de foranstaltninger der skal iværksættes nogle, som skal hjælpe databehandleren med at opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger fra de registrerede. Disse foranstaltninger er ikke overlappende med sikkerhedsforanstaltningerne i artikel 32. Et andet eksempel kan findes i artikel 24, stk. 1 hvor foranstaltninger har til formål at være i stand til at påvise, at behandling er i overensstemmelse med forordningen. Også disse foranstaltninger må siges at være nogle andre end sikkerhedsforanstaltningerne fra artikel 32.

Hvad ligger der så i tekniske og organisatoriske foranstaltninger, som kan understøtte databeskyttelse gennem design? Begrebet privacy by design stammer fra Ann Cavoukian, som i 90'erne opstillede syv principper, der skulle bruges som guideline, når der blev designet it-systemer, der skulle behandle personoplysninger. Disse principper blev vedtaget i en resolution på Datatilsynenes 32 internationale konference i 2010 og det danske Datatilsyn henviser til dem:

- Proaktiv, ikke reaktiv
- Privacy som standardindstilling
- Privacy skal være indlejret I systemet
- Der skal være fuld funktionalitet
- Beskyttelse i hele livscyklussen
- Synlighed og trasparens
- Brugeren i centrum

Princip nummer tre giver en god indikation af, at lovgiver har tænkt på disse principper i og med at dette er integreret direkte i artikel 25, stk. 2. Som det fremgår, er disse principper ikke nødvendigvis sikkerhedsforanstaltninger med i stedet designforanstaltninger. Det er f.eks. ikke en sikkerhedsforanstaltning at indlejre noget i en teknologi. Det er en designforanstaltning.

Ud over Ann Cavoukians principper findes der flere andre sammenstillinger af designprincipper, som man kunne tage udgangspunkt i for at kortlægge det selvstændige materielle indhold i DPbD, f.eks. Hoepmans designstrategier, som ENISA har taget udgangspunkt i en rapport, eller Borking and Blarkom om privatlivsfremmende teknologier, som understøtter både/eller sikkerhed og design. Det vil imidlertid være for omfattende at berøre alle disse tilgange i dette høringssvar. Cavoukians principper er imidlertid

tilstrækkeligt til at illustrere at DPbD har et materielt selvstændigt indhold, der er forskelligt fra sikkerhedsforanstaltninger.
JM anfører, at artikel 29-gruppen i flere udtalelser har stillet krav om designforanstaltninger. Som eksempel har artikel 29-gruppen i Opinion 01/2015 om privacy i droner netop opfordret til: "Embed privacy friendly design choices and privacy friendly defaults as part of a privacy by design approach". Alle de udtalelser, som involverer noget om design, er så vidt vides fra efter januar 2012, hvor første udkast til forordningen blev offentliggjort, og i hvert fald efter princippet blev skabt af Cavoukian i 90'erne. Man kan sige, at artikel 29-gruppen med udtalelsen har taget forskud på glæderne ved artikel 25 inden den fik virkning.

Pointen er ikke en lang juridisk akademisk diskussion af, om hvorvidt en given passende teknisk eller organisatorisk foranstaltning er en designforanstaltning eller en sikkerhedsforanstaltning. Pointen er, at hvis designforanstaltninger ikke i sig selv tillægges et materielt indhold, overser man alle de foranstaltninger, som kan siges alene at være designmæssige, og dermed at have deres retlige grundlag i artikel 25 uden at være sikkerhedsmæssige med retligt grundlag i artikel 32. Man bruger så at sige kun halvdelen af værktøjerne i værktøjskassen. Hvis der derimod tillægges et selvstændigt materielt indhold til DPbD, skabes der en passende teknisk og organisatorisk understøttelse af f.eks. dataklassifikation, dataportabilitet og oplysningspligt.

RfDS finder, at JM har overset, at der ligger et materielt indhold i artikel 25, som defineres af de brede mængde af muligheder, der er for at designe beskyttelse af personoplysninger ind i sine løsninger. Hvilke designmæssige foranstaltninger der konkret skal iværksættes, afhænger ligesom foranstaltningerne i artikel 32 af de konkrete behandlinger m.v. Men artikel 25 indebærer en pligt til at overveje et mulighedsrum af designmæssige foranstaltninger som ligger ud over, hvad der kan ske i medfør af artikel 32. Mulighedsrummet fastlægges ligesom for artikel 32 af konkrete vurderinger og af praksis. Ann Cavoukians principper er en del af dette designmæssige mulighedsrum. De designmæssige foranstaltninger kan bl.a. tilføjes til værktøjskassen omtalt i høringsudkastet pp. 184-185.

Rådet står naturligvis til rådighed for en uddybelse af ovenstående bemærkninger.

Med venlig hilsen

Bestyrelsen
Rådet for Digital Sikkerhed