DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Justitsministeriet
Att.:jm@jm.dk
Slotsholmsgade 10
1216 København K

Den 26. august 2019

Høringssvar til udkast til bekendtgørelse samt vejledning vedrørende databeskyttelseslovens § 3 stk.9 (krigsreglen)

Dansk Erhverv og IT-Branchen har modtaget Justitsministeriets udkast til bekendtgørelse samt medfølgende vejledning om databeskyttelseslovens §3 stk.9 (krigsreglen) i høring. Vi har følgende bemærkninger til materialet:

Generelle bemærkninger

I modsætning til tidligere, hvor hver enkelt myndighed mere eller mindre kunne komme med sin egen fortolkning af den daværende krigsregel i "lov om behandling af personoplysninger" § 41, henlægger databeskyttelsesloven beslutningen om, hvorvidt et system er omfattet af krigsregen eller ej, til Justitsministeriet. Samtidig indeholder vejledningen relativ klare retningslinjer og processer for myndighedernes håndtering og stillingtagen til krigsreglen.
Begge dele ser Dansk Erhverv og IT-Branchen meget positivt på, idet kommende IT-udbud desangående må formodes at være mere ensartede.

Dansk Erhverv og IT-Branchen ser det desuden som meget positivt, at det klart fremgår af vejledningen, at krigsreglen har fokus på "statens sikkerhed" og ikke "behandlingssikkerhed", og at der skal meget til, før man kan tale om statens sikkerhed. Hvis denne intention fastholdes, bør listen over systemer, der alene må opbevares i Danmark, forblive kort.

Endelig ser Dansk Erhverv og IT-Branchen det som meget positivt, at vejledningen har en mere pragmatisk holdning til support/kiggeadgang fra andre lande til et system omfattet af krigsreglen. Denne tilgang vil gøre databehandlingen af systemerne langt mere praktisk orienteret uden det går ud over statens sikkerhed.

Dansk Erhverv og IT-Branchen er dog bekymrede for, at den nye vejledning kan føre til en liste der vokser dynamisk i takt med at flere systemer kommer i genudbud, stik imod hensigten med databeskyttelsesloven, ligesom vi flere steder i vejledningen har brug for yderligere afklaring eller eksempler for at sikre at vejledningen forstås ens af alle relevante aktører.

Specifikke bemærkninger

Indledende visitation

Det er uklart hvad definitionen af "statens sikkerhed" er – hvad kan true statens sikkerhed og hvad har været bevæggrundene herfor. Det er svært at forstå hvad de bagvedliggende overvejelser er og det er uklart hvornår noget truer statens sikkerhed.

I afsnit 3.4 oplistes otte spørgsmål, som angives som værende relevante ved vurderingen af, om et system er omfattet af krigsreglen. Det fremgår ikke af vejledningen, hvorfor netop disse 8 spørgsmål er relevante for statens sikkerhed, og dermed kravet om opbevaring i Danmark, herunder hvordan de identificerede risici mindskes ved et krav om opbevaring i Danmark.

Dansk Erhverv og IT-Branchen vurderer, at mange myndigheder ved en gennemgang af de otte spørgsmål vil score deres it-systemer i rød, selvom it-systemerne ikke umiddelbart vil ende på listen over systemer der skal opbevares i Danmark. Det kan skabe en uønsket forventning i flere myndigheder om at deres systemer falder ind under krigsreglen, hvilket kan være med til at trække afgørelsen i langdrag.

For både at spare Justitsministeriet for de mange henvendelser og for at sikre hurtigere processer, bør de otte punkter uddybes yderligere, så kun de relevante systemer skal forbi en vurdering i Justitsministeriet. Dette kan også sikres ved at udbygge vejledningen med eksempler på, hvordan de otte spørgsmål er blevet besvaret for udvalgte systemer som Justitsministeriet har vurderet i forhold til krigsreglen. Det vil i så henseende være nyttigt med eksempler på, hvorfor systemer netop *ikke* er blevet omfattet af krigsreglen, såvel som det modsatte.
Et andet tema er hvorvidt dele af et system kan være omfattet af krigsreglen. Her savnes eksempler på hvordan det i givet fald skal gribes an. Skal reglerne forstås sådan, at man ved ethvert indkøb af et system skal igennem en større overvejelse omkring hvorvidt systemet skal splittes op i forskellige dele der henholdsvis indeholder ufarlige data og data der er omfattet af krigsreglen.

Det bør endvidere fremgå af vejledningen, i hvilket omfang myndighederne skal orientere Justitsministeriet om den indledende visitation, eller om det vil det være op til Datatilsynet, som tilsynsførende myndighed, at påse om krigsreglen er overholdt.

Opbevaring vs. Behandling

Som indledningsvis nævnt, skal krigsreglen udelukkende sikre, at personoplysninger i visse it-systemer opbevares på servere i Danmark. Reglen skal ikke regulere behandlingen af personoplysninger. Alligevel omhandler afsnit 4 bestemmelser om supportadgang til systemerne udenfor Danmark. Det skaber en usikkerhed i forhold til forståelse af begrebet opbevaring.

Som Databeskyttelsesloven er formuleret, synes Justitsministeriet alene at have beføjelse til at fastsætte regler for, hvilke it-systemer, der ikke må opbevares uden for Danmark af hensyn til statens sikkerhed - ikke at have hjemmel til at fastsætte krav til behandlingssikkerhedsforanstaltninger.

Det vil være hensigtsmæssigt, hvis der i vejledningen bliver indsat et separat afsnit om fortolkning af begrebet "opbevaring".

Endvidere bør det i afsnit 4 gøres helt klart, om det skal forstås som en *mulighed* eller en *pligt* for myndigheden, hvorvidt de skal drøfte krav til behandlingssikkerhedsforanstaltninger med Justitsministeriet, og om Justitsministiet har eller ikke har beføjelser til at fastsætte krav til foranstaltninger vedrørende behandlingssikkerhed, samt hvilke kriterier, som vil være relevante for vurderingen af, om denne "kiggeadgang" kan tillades.

Vejledningen definerer ikke nærmere, hvad der menes med "kiggeadgang". En uddybning af dette begreb ville være ønskelig.

Vurdering af konkrete systemer
Justitsministeriet har i vejledningen anvendt eksempler på systemer der er kommet på listen og to systemer der ikke er kommet på listen. Dette er en rigtig god måde at konkretisere vejledningen på, og kunne med fordel udbygges for at sikre en bedre forståelse for krigsreglen.

Det vil først og fremmest være en god rettesnor for anvendelse af vejledningen, hvis det for de omtalte systemer blev gennemgået, hvordan de otte spørgsmål fra afsnit 3.4 konkret er blevet anvendt på disse systemer

Det vil endvidere skabe en større gennemsigtighed og forståelse for krigsreglen, hvis Justitsministeriet vil offentliggøre en samlet liste over alle de eksisterende it-systemer Justitsministeriet har vurderet ved udformning af krigsregel-bekendtgørelsen. Hvis vi ikke har den samlede liste, kan der opstå tvivl om, hvorvidt eksisterende systemer med persondata uden for Danmark er lovlige. Det er f.eks. uklart, hvorvidt Justitsministeriet har foretaget en vurdering af alle offentlige centrale it-systemer, der anvendes i dag, således at listen pt. skal anses som udtømmende, eller hvorvidt der kun er vurderet en mindre del af de centrale it-systemer.

Hvis der kun er vurderet en delmængde, er det særlig relevant at få klarhed omkring de systemer der er krævet opbevaret i Danmark efter den gamle krigsregel, som fx DFDG-databasen. Er der foretaget en ny vurdering af disse systemer og hvilke krav er gældende for systemerne?

Hvornår finder vejledningen og den nye krigsregel anvendelse?
Det fremgår af vejledningen afsnit 3.1 at vejledning skal følges, når vedkommende minister overvejer at indkøbe et nyt it-system, en ny it-infrastruktur eller lign., ligesom vejledningen skal følges ved (gen)udbud eller outsourcing af eksisterende it-systemer eller dele heraf.

Der mangler dog i vejledningen en tilkendegivelse af, fra hvornår vejledningen er gældende. Er det fra ikrafttrædelse af bekendtgørelsen eller fra ikrafttrædelse af databeskyttelsesloven? Dette har indflydelse på, hvilke regler der gælder for it-systemer anskaffet i tidsperioden mellem databeskyttelseslovens ikrafttrædelse og bekendtgørelsens ikrafttrædelse.

Endvidere: er det egentlig muligt at opretholde "den gamle krigsregel" for it-systemer indkøbt via EU-udbud før databeskyttelseslovens ikrafttrædelse/bekendtgørelsens ikrafttrædelse? GDPR - og

undtagelse herfra begrundet i hensyn om varetagelse af statens sikkerhed - må gælde for alle it-systemer, uanset hvornår it-systemerne er indkøbt. Dvs. hensyn til statens sikkerhed må vel skulle vurderes konkret på baggrund af det til enhver tid gældende teknologiske stade. I modsat fald vil man udstrække rækkevidden af "den gamle krigsregel" i mange år frem – en gammel krigsregel, som man netop vil forlade, fordi reglen ikke er tidssvarende pga. den teknologiske udvikling.

Hvis man holder fast i, at den gamle krigsregel skal vedblive at gælde for it-systemer indkøbt via EU-udbud før databeskyttelseslovens ikrafttrædelse/bekendtgørelsens ikrafttrædelse, så bør forbuddet mod behandling uden for Danmark begrænses til kun at gælde "opbevaring" og ikke andre behandlinger som fx. support/kigge-adgang fra et andet land end Danmark. Dette bør fremgå tydeligt af vejledningen.

Endelig mangler der klarhed om i hvilket omfang datatilsynets tidligere praksis om "krigsreglen" fortsat er relevant. Skal vejledningen fx forstås således, at Datatilsynets udtalelse til ATP om mulighed for overførsel af data ikke længere er relevant?

Opgavefordeling mellem myndighed, ressortministerium og Justitsministeriet

Opgavefordelingen mellem resortmyndigheden på den ene side, og underliggende myndigheder, kommuner, regioner mv. på den anden side er uklare. Her tænkes især på punkt 3.2 -3.4. Justitsministeriet opfordres til at tydeliggøre dette.

Vejledningen giver indtryk af, at den enkelte underliggende myndighed selv skal foretage vurderinger og tilvejebringe oplysninger - og alligevel er det ressortmyndigheden der skal henvende sig og indgå i dialog med Justitsministeriet om "sine overvejelser". Det forekommer modstridende.

Vi har for nuværende ikke yderligere bemærkninger, men står gerne til rådighed for evt. uddybende kommentarer.

Med venlig hilsen,

Sven Petersen
Erhvervsjuridisk fagchef
Dansk Erhverv

Martin Jensen Buch
Chefkonsulent
IT-Branchen