Indholdsfortegnelse

3F	2
Analog Netværket	3
ATP	4
Borger 1	7
Borger 2	9
Borger 3	20
Borger 4	30
Borger 5	32
Borger 6	37
Dansk Erhverv	40
Dansk Industri	44
Dansk Selskab for Almen Medicin	53
Dansk Socialrådgiverforening	78
Danske Advokater	84
Danske Professionshøjskoler	85
Danske Regioner	87
Danske Universiteter	94
Dataetisk Råd	108
Datatilsynet	119
Domstolsstyrelsen	139
Edora A/S	141
EG Danmark	148
F&P	152
Faxe Kommune	153
Finanstilsynet	156
Forbrugerrådet Tænk	158
FSR Danske Revisorer	161
GRO Capital A/S og QUMEA Danmark	167
HK Danmark	170
IDA Teknologivurdering	181
Ingeniørforeningen IDA	185
Institut for Menneskerettigheder	188
IT-Branchen	199
IT-Politisk Forening	204
Justitia	209
KL	216
KOMBIT	222
Københavns Kommune	225
Priway ApS	232
Rigsrevisionen	238
Rådet for Digital Sikkerhed	240
Ældresagen	244
Aalborg Kommune	247
Aarhus Kommune	252

Til: jonmei@digst.dk, kahevi@digst.dk, emimol@digst.dk, leaomd@digst.dk
Cc: thomas.bentsen@3f.dk (Thomas Bentsen, A-kassen), simon.redder@3f.dk (Simon Redder Momsen, A-kassen), susanne.a@3f.dk (Susanne Refslund Andresen, A-kassen), michael.kristiansen@3f.dk (Michael Kristiansen, A-kassen), jette.hvarre@3f.dk (Jette Tingleff Hvarre, A-kassen)
Fra: Vibeke Sejling-Handberg, A-kassen (vibeke.sejling-handberg@3f.dk)
Titel: VS: [Ekstern] Høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger
Sendt: 12-10-2026 09:23
Bilag: image001.png;

Hermed 3F's svar på høring om offentlige myndigheder og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Vi finder det er godt med en generel hjemmel til anvendelse af AI-systemer, men vil gerne have det tydeligere beskrevet om a-kasser falder ind under denne hjemmel.

Det er beskrevet at det er usikkert, hvor stor den menneskelige involvering skal være, førend der er tale om beslutningsstøtte og ikke fuldautomatiske afgørelser eller tiltag. Dette er ikke fastlagt klart i praksis, og det forventes derfor at det vil blive præciseret nærmere i fremtidig praksis. Vi finder det betænkeligt, at der gives hjemmel, hvor der ikke er en tydeligere præcisering af, hvad der gives hjemmel til, og at dette først forventes præciseret i praksis efterfølgende. Vi finder det endvidere ønskeligt, at der er en nærmere beskrivelse af, hvor meget der kan anvendes profilering, samt til hvilke formål.

De bedste hilsner

Vibeke Sejling-Handberg
Jurist
Faglig Fælles A-kasse

Faglig Fælles A-kasse

Kampmannsgade 4
1604 København V

Mail: vibeke.sejling-handberg@3f.dk
Telefon: 6025 3450

Århus, 5. september, 2026

Høringssvar fra foreningen Analog Netværket,

-interesseorganisation for de ca. 20 % af befolkningen, der er enten helt analoge, eller har udfordringer med det digitale eller med digitalisering generelt.

Analog Netværket takker for muligheden for at afgive høringssvar i denne vigtige sag.

Vi kan på ingen måde støtte forslaget, da det åbner op for en lang række problematikker - som altså generelt kan undgås, ved ikke at benytte AI i forvaltningen.
Generelt mener vi, er digitaliseringen gået for stærkt, så man begår alverdens fejl -og bruger skattekroner- uden den store eftertanke, og uden at vente på at disse fejl udbedres, eller sørger for at alle borgere kan følge med i det høje tempo.

Vi mener derfor, at man bør overveje tempoet for digitaliseringen meget grundigt -og ikke kaste sig ud i nye digitale eksperimenter -samt tænke analoge borgere ind fra start, og ikke som appendix eller som en "hovsa-ting"; og afvente andre landes erfaringer med brug af AI, så vi undgår at begå de samme begynderfejl. Man bør tage tanken om AI op til revision, når der foreligger et oplyst grundlag at træffe beslutninger på baggrund af: Den nødvendige reflektion og en befolkningsmæssig opbakning.

Kritiske bemærkninger:
- -Kan en borger, der er fritaget fra digital post, og som ikke kan få mitID, blive delvist sagsbehandlet af en AI?
  Eller kan man forestille sig, at man kan blive fritaget som analog/ikke-digital borger? Vi mener det bør være en ret, at kunne få hele sagsbehandlingen udført af et menneske, uden kunstig "beslutningsstøtte".
- -Det svækker generelt tilliden til myndighederne, hvis AI bruges i sagsbehandlingen, når man har krav på ikke-digitale løsninger andetsteds -også selvom man ikke er fritaget.
- -Tanken om at lave fælles regler bakker vi sådan set op om, men vi noterer os at der IKKE er lagt op til fælles retningslinjer, hvis de enkelte ministre selv kan bestemme, hvordan deres ministerier bruger AI. Vi appellerer til at AI på ingen måde bruges, når det gælder indflydelse på menneskers forhold og skæbne.

Konklusion.
Dette lovforslag går i den forkerte retning, og vil skabe endnu større ulighed mellem analoge og digitale borgere. Intentionen om regulering er god, men når der alligevel bliver åbnet op for muligheden for at benytte kunstig intelligens på borgerne, vil det altid være en glide-bane.

På vegne af Analog Netværket og de analoge borgere,
Lukas Eisenberg og Anders B.

KOPI

Digitaliseringsstyrelsen
Landgreven 4
1017 København K

Att.: Fuldmægtig Jonathan Meijer, jonmei@digst.dk, Fuldmægtig Lea Marie Omdahl, leaomd@digst.dk

12. oktober 2026

Høringssvar vedrørende forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

ATP
Kongens Vænge 8,
3400 Hillerød

Tlf.: 70 11 12 13
Fax: 48 20 48 02

www.atp.dk

CVR-nr.: 43405810

Telefontid:
Mandag - Torsdag: 8.00-16.00
Fredag: 8.00-15.30

Arbejdsmarkedets Tillægspension (ATP) afgiver hermed bemærkninger til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Høringssvaret afgives på vegne af ATP og de af ATP administrerede ordninger, herunder Udbetaling Danmark (UDK) og Arbejdsmarkedets Erhvervssikring (AES) (samlet benævnt "ATP").

ATP noterer sig, at lovforslaget er sendt i fornyet høring, efter denne blev afbrudt tidligere i 2026 grundet udskrivelsen af folketingsvalg. ATP genfremsætter derfor i det væsentlige sine tidligere bemærkninger, idet disse vurderes fortsat at være relevante. ATP har samtidig noteret sig de ændringer og præciseringer, der er foretaget i lovforslaget.

1. Overordnede bemærkninger

ATP har ved lov ansvar for at administrere en række centrale velfærdsydelser og er i den forbindelse forpligtet til løbende at udvikle og effektivisere administrationen til gavn for borgerne, opdragsgiverne og samfundet. AI-systemer kan understøtte mere effektive og kvalificerede sagsprocesser. Det er samtidig afgørende for ATP, at anvendelsen sker inden for klare retlige rammer og med respekt for borgernes data og den tillid, der er knyttet til den offentlige forvaltning af personoplysninger.

ATP finder det positivt, at lovforslaget etablerer et generelt databeskyttelsesretligt hjemmelsgrundlag for offentlige myndigheders og organers udvikling og anvendelse af AI-systemer som led i deres allerede fastlagte opgavevaretagelse. Det kan skabe større retlig klarhed, ensartethed og forudsigelighed og ikke mindst mindske behovet for, at der skal etableres særskilte hjemler for den enkelte ordning eller myndighed.

ATP bemærker samtidig, at databeskyttelsesforordningen og databeskyttelsesloven er teknologineutrale. Anvendelsen af AI efter ATP's vurdering derfor bør kunne ske inden for de eksisterende databeskyttelsesretlige rammer, når den konkrete behandling sker inden for rammerne af den relevante opgavehjemmel og de databeskyttelsesretlige krav, herunder krav om behandlingsgrundlag, nødvendighed, proportionalitet og passende garantier.

2. Den generelle hjemmel (§ 3, stk. 1)
ATP finder det positivt, at lovforslaget og bemærkningerne præciserer, at hjemlen i § 3, stk. 1 omfatter behandling af alle kategorier af personoplysninger i AI-systemer, herunder følsomme personoplysninger og oplysninger om strafbare forhold efter hhv. artikel 9 og 10 i databeskyttelsesforordningen.

ATP noterer sig, at den foreslåede hjemmel ikke ændrer på kravene i anden lovgivning, herunder forvaltningsretlige regler, tavshedspligt, regler om videregivelse, samkøring og tredjelandsoverførsler.

3. Beslutningsstøtte og fuldautomatiske afgørelser (§ 2, nr. 4, og § 3, stk. 1)
ATP finder det tillige positivt, at lovforslaget indeholder en definition af beslutningsstøtte og nu nærmere beskriver kravet om reel menneskelig involvering.

ATP opfordrer til, at den planlagte vejledning indeholder konkrete eksempler på indretning af arbejdsgange og kontrolforanstaltninger, som kan understøtte den reelle og selvstændige faglige vurdering. Vejledningen bør samtidig understrege, at foranstaltningerne skal være risikobaserede og afspejle den konkrete AI-anvendelses betydning for de registrerede.

4. Følsomme oplysninger, oplysninger om strafbare forhold og passende garantier (§ 3, stk. 2)
ATP forstår § 3, stk. 2 således, at der skal foretages en konkret vurdering af, om gældende sektorlovgivning indeholder tilstrækkelige passende og specifikke garantier når behandlingen foretages ved brug af et AI-system. Er dette ikke tilfældet ved behandling af følsomme personoplysninger eller oplysninger om strafbare forhold, skal de nødvendige supplerende garantier fastsættes ved bekendtgørelse.

ATP finder, at det hensigtsmæssigt, at det præciseres i lovbemærkningerne, at § 3, stk. 2 ikke finder anvendelse, hvis et AI-system hverken udvikles med henblik på behandling af følsomme eller strafbare oplysninger, og det heller ikke er formålet at anvende systemet til sådan behandling. I praksis kan der forekomme tilfælde, hvor sådanne oplysninger sporadisk optræder, fx i fritekstfelter eller som utilsigtet del af inputdata, fx fra en borger, uden at dette udgør et tilsigtet eller systematisk behandlingsformål. Efter præciseringen af § 3, stk. 2 vurderes det i disse situationer ikke i sig selv at udløse krav om fastsættelse af en ressortbekendtgørelse, forudsat at behandlingen håndteres inden for rammerne af de almindelige databeskyttelsesretlige krav, herunder passende tekniske og organisatoriske foranstaltninger.

5. Krav til vurdering af foranstaltninger og passende garantier (§ 3, stk. 2)
ATP opfordrer til, at vejledningsmaterialet bidrager til hvordan vurderingen af, om der foreligger tilstrækkelige foranstaltninger og passende garantier, skal gennemføres i praksis. På flere af de områder, som ATP administrerer, indeholder særlovgivningen ikke eksplicitte bestemmelser om behandling af følsomme eller strafbare oplysninger eller om krav til konkrete garantier. Der vurderes derfor at være behov for at få yderligere præciseret, hvordan vurderingen skal foretages, og hvilke metodiske rammer der skal anvendes.

ATP anbefaler endvidere, at der udarbejdes et fælles foranstaltningskatalog eller anden fælles ramme, som kan anvendes på tværs af ressortområder. Rammen bør angive relevante minimumstemaer og samtidig muliggøre en risikobaseret graduering efter den

konkrete anvendelse. Dette kan understøtte ensartethed og undgå, at der udvikles unødigt forskellige krav til sammenlignelige AI-anvendelser.

6. Begrænsninger i de registreredes rettigheder (§ 4)
ATP noterer sig, at § 4 giver mulighed for, at ressortministrene inden for rammerne af databeskyttelsesforordningens artikel 23 ved bekendtgørelse kan fastsætte helt eller delvise begrænsninger af bestemte registreredes rettigheder. ATP anerkender, at AI-systemers tekniske opbygning i konkrete tilfælde kan gøre det vanskeligt at imødekomme navnlig anmodninger om indsigt eller sletning.

ATP opfordrer til, at det tydeliggøres hvilke kriterier, der skal lægges til grund ved vurderingen af nødvendighed og proportionalitet, og hvilke alternative og kompenserende garantier der skal træde i stedet for de begrænsede rettigheder.

Det foreslås desuden præciseret, hvordan kravet om forudgående inddragelse af Datatilsynet skal gennemføres i praksis, og hvilken betydning Datatilsynets udtalelse har.

6. Afsluttende bemærkninger
ATP vurderer samlet, at lovforslaget vil reducere den retlige usikkerhed om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning. Det vil samtidig gøre det muligt i højere at anvende AI i det offentlige, hvor det er relevant og kan skabe værdi, herunder effektivere administrationen.

ATP står naturligvis til rådighed for eventuelle spørgsmål til høringssvaret og i øvrigt.

Med venlig hilsen

Maria Damborg Hald
Koncerndirektør
Borger & Velfærd

Pernille Vastrup
Koncerndirektør, CFO
Corporate Functions

Til: jonmei@digst.dk (Jonathan Kirkegaard Meijer)
Fra: Jonathan Kirkegaard Meijer (jonmei@digst.dk)
Titel: VS: Høringsvar for det nye udkast til lov om offentlige myndigheders udvikling og anvendelse af AI-systemerDIGST (Id nr.: 2947178)
Sendt: 23-10-2026 15:08

Til: DIGST POST (digst@digst.dk)
Fra: Alex Gumieniak Psychologica.dk (alex.gumieniak@me.com)
Titel: Høringsvar for det nye udkast til lov om offentlige myndigheders udvikling og anvendelse af AI-systemer
Sendt: 19-09-2026 01:57

Til Digitaliseringsstyrelsen,

Undertegnede, cand.psych., skal herved fremkomme med retssikkerhedsmæssige, compliance-mæssige og EU-retlige bemærkninger til det fremsendte lovudkast. Mine bemærkninger koncentrerer sig om de systemiske risici, som udkastets §§ 3 og 4 rejser i forhold til det menneskelige sind, kognitive funktionsnedsættelser og psykisk sårbarhed.

1. Konflikt med GDPR artikel 22 og tilsidesættelse af officialprincippet (§ 3)
Det må lægges til grund, at den foreslåede generelle hjemmel i § 3, stk. 1, til profilering og automatiseret sagsbehandling, udfordrer rammerne for GDPR artikel 22. Efter EU-retten har borgeren en grundlæggende ret til ikke at blive underlagt rent automatiserede afgørelser, medmindre der foreligger specifikke og præcise nationale retsgarantier.

Lovudkastet baserer sig på en forudsætning om, at alle borgere besidder den samme kognitive kapacitet til at gennemskue algoritmiske systemer. Borgere med kognitive funktionsnedsættelser (herunder neurodivergens eller svære belastningsreaktioner) udviser en anden kognitiv profil end den standardiserede gennemsnitsborger, som offentlige AI-modeller trænes på. En algoritmisk standardisering risikerer at føre til systematiske bias og fejlvisninger over for dette digitale sind, da AI mangler den menneskelige intuition til at kompensere for kognitive barrierer. Dette berører forvaltningens officialprincip, og afgørelser truffet på baggrund af denne hjemmel vil være sårbare over for omstødelse ved domstolene.

2. Konflikt med EU's AI Act og vanskeliggørelse af retsbeskyttelse (§ 4)
Lovudkastets § 4 tillader, at væsentlige begrænsninger af borgerens indsigts- og gennemsigtighedsrettigheder kan fastsættes administrativt via ministerielle bekendtgørelser.

Dette strider direkte imod hensigten i EU's AI Act, som klassificerer offentlig sagsbehandling via AI som et højrisikoområde, der kræver streng gennemsigtighed og obligatorisk menneskeligt tilsyn (human oversight). For en borger med et kognitivt udfordret sind skaber det en væsentlig retssikkerhedsmæssig barriere, hvis myndigheden administrativt kan begrænse indsigten i algoritmens datagrundlag. At uddelegere begrænsninger af fundamentale EU-retlige gennemsigtighedskrav til bekendtgørelser uden direkte parlamentarisk kontrol øger den statslige ansvarsrisiko for traktatbrudssager.

3. Procedural mangel i forhold til EU's Web-tilgængelighedsdirektiv
Det påpeges desuden, at de nuværende rammer for høringen via Høringsportalen ikke opfylder EU-rettens krav om universelt design og kognitiv tilgængelighed (jf. Europa-Parlamentets og Rådets direktiv 2016/2102). Lovudkastets komplekse juridisk-tekniske sprog udelukker i praksis den målgruppe, hvis rettigheder indskrænkes, fra at deltage ligeværdigt i den demokratiske proces. Høringsprocessen lider derved af en procedurel mangel.

4. Konklusion og anbefaling
Lovudkastet bør i sin nuværende form justeres før fremsættelse for at sikre EU-retlig compliance.

Det henstilles, at der i selve lovteksten indføres et absolut "Analogt Sikkerhedsnet" for at imødegå statsligt ansvar. Det bør være en ufravigelig borgerret, at:

- * Borgere med kognitive eller psykiske funktionsnedsættelser har en ubetinget ret til altid at kræve analog, menneskelig sagsbehandling og menneskeligt tilsyn (human oversight) i overensstemmelse med AI Act.
- * Der ydes personlig, håndholdt hjælp til udøvelse af den registreredes indsigtsret efter databeskyttelsesforordningen (GDPR).

Med venlig hilsen,
Alex Gumieniak
Cand.psych.

Sendt fra min iPad

Høringssvar vedrørende forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Høring:	Nr. 71477
Dato:	14. september 2026
Version:	Udvidet høringssvar - version 3
Afsender:	Johnny Rivli

Jeg fremsender hermed bemærkninger til det fremsendte lovforslag.

Særligt fremhævede forhold

Ved en nærmere sammenligning af lovudkastets forskellige afsnit og den tidligere høringsrunde er der identificeret flere forhold, som efter min opfattelse kræver en udtrykkelig afklaring før fremsættelse: en intern modstrid mellem "kan" og "skal" ved særlige beskyttelsesforanstaltninger, en fejlagtig henvisning til GDPR artikel 13, stk. 4, et muligt overgangsgab frem til centrale højrisikokrav i EU's AI-forordning bliver anvendelige, samt manglende krav om dokumentation af den menneskelige kontrol.

Lovforslaget vedrører et område med meget vidtrækkende konsekvenser for borgernes retssikkerhed. Der er ikke alene tale om regulering af et nyt teknisk redskab, men om etablering af et generelt retsgrundlag for, at offentlige myndigheder og organer kan anvende allerede indsamlede personoplysninger til udvikling og anvendelse af AI-systemer, herunder profilering og beslutningsstøtte.

Netop derfor bør lovgivningen efter min opfattelse indeholde væsentligt stærkere, direkte og kontrollerbare rettighedsgarantier end det foreliggende forslag.

Kort overblik over de væsentligste forhold

Intern modstrid om følsomme data.

§ 3, stk. 2, siger "kan", mens et andet afsnit i lovmaterialet fortsat siger "skal" om fastsættelse af særlige beskyttelsesforanstaltninger. Retstilstanden bør være entydig før fremsættelse.

Fejl i GDPR-henvisningen.

Bemærkningerne knytter en lovbaseret undtagelse fra oplysningspligten til artikel 13, stk. 4, selv om denne bestemmelse alene vedrører tilfælde, hvor den registrerede allerede kender oplysningerne. Den relevante lovbaserede undtagelse findes under andre betingelser i artikel 14, stk. 5, litra c.

Et muligt overgangsgab.

Den danske hjemmelslov kan træde i kraft, før centrale højrisikokrav i EU's AI-forordning finder fuld anvendelse. Der bør derfor være nationale overgangsværn.

Menneskelig kontrol uden sikkert bevisspor.

Lovbemærkningerne kræver reel og meningsfuld menneskelig kontrol, men gør ikke logning, dokumentation af afvigelser eller identifikation af beslutningstager til generelle lovkrav.

En meget bred generel hjemmel.

§ 3 skal kunne anvendes på tværs af meget forskellige myndighedsområder. Det skærper behovet for klare lovbestemte minimumsgarantier om datatyper, kvalitet, bias, sporbarhed og kontrol.

Rettigheder versus systemdesign.

§ 4 åbner for begrænsning af registreredes rettigheder i situationer, hvor efterlevelse kan være vanskelig eller påvirke systemets præcision. Udgangspunktet bør være, at teknologien indrettes efter rettighederne - ikke omvendt.

Langsigtet forskydning fra sektorregler til generallov.

Bemærkningerne åbner for, at specifikke sektorhjemler senere kan erstattes af den generelle AI-hjemmelslov. Det gør en bindende evaluering og parlamentarisk opfølgning nødvendig.

1. En meget bred generel hjemmel kræver tilsvarende stærke generelle værn

Lovforslagets grundmodel er, at én generel lov skal kunne danne supplerende behandlingsgrundlag for AI-anvendelse på tværs af en meget stor del af den offentlige sektor.

Dette indebærer en principiel forskydning.

Hvor nye og indgribende anvendelser af personoplysninger ellers ofte vil give anledning til en konkret politisk og lovgivningsmæssig vurdering, etableres med lovforslaget en bred forhåndshjemmel, som efterfølgende kan anvendes inden for mange forskellige sektorer og myndighedsområder.

Denne konstruktion kan være administrativt effektiv. Men effektivitet må ikke stå alene.

Jo bredere hjemlen er, desto stærkere bør de fælles og lovfæstede minimumsgarantier være.

Det modsatte risikerer at føre til, at meget væsentlige retssikkerhedsspørgsmål i praksis flyttes fra Folketingets konkrete behandling til administrative vurderinger, ressortministerier og bekendtgørelser.

2. Ændringen fra "skal" til "kan" i § 3, stk. 2 - og en intern modstrid i lovbemærkningerne

Det foreliggende udkast ændrer den tidligere konstruktion vedrørende særlige beskyttelsesforanstaltninger omkring følsomme personoplysninger.

Hvor det tidligere udkast anvendte en pligtbestemmelse, hvorefter vedkommende minister "skal" fastsætte specifikke beskyttelsesforanstaltninger i relevante tilfælde, anvender det nye forslag formuleringen "kan".

På side 32 understreges det desuden, at der med lovforslaget ikke etableres en generel forpligtelse til at fastsætte yderligere foranstaltninger ved bekendtgørelse.

Imidlertid står der på side 50 under vurderingen af digitaliseringsklar lovgivning, at vedkommende minister og Domstolsstyrelsen **"skal fastsætte specifikke foranstaltninger"** i de relevante tilfælde.

Lovbemærkningerne giver dermed ikke et entydigt svar på, om udstedelse af særlige sektorbestemte foranstaltninger er en retlig pligt eller alene en bemyndigelse. Det bør afklares og teksten bringes i indbyrdes overensstemmelse før fremsættelse.

Der er tale om behandling af de mest følsomme kategorier af personoplysninger, herunder oplysninger om eksempelvis helbred og genetiske forhold samt oplysninger om strafbare forhold. Netop her bør retstilstanden være utvetydig.

Efter min opfattelse bør loven som minimum indeholde obligatoriske fælles krav til behandling af følsomme oplysninger i forbindelse med AI. Disse bør ikke alene være mulige at fastsætte senere; de bør gælde fra lovens ikrafttræden.

3. Historiske personoplysninger må ikke blive et permanent råstoflager til nye AI-formål

Lovforslaget giver mulighed for, at personoplysninger fra historiske og afsluttede sager kan indgå i udvikling og træning af AI-systemer, når de øvrige databeskyttelsesretlige betingelser er opfyldt.

Det er et meget væsentligt principielt spørgsmål.

En borger kan have afgivet oplysninger til en myndighed i en bestemt sammenhæng og med en legitim forventning om, at oplysningerne blev anvendt til netop denne myndighedsopgave.

År senere kan de samme oplysninger efter den foreslåede model få en ny funktion som træningsgrundlag for et AI-system.

At en oplysning fortsat lovligt opbevares, bør ikke i sig selv gøre den til et teknologisk råstof, der automatisk er egnet til nye analyse- og træningsformål.

Der bør derfor indføres en skærpet nødvendighedstest for genanvendelse af historiske personoplysninger til AI-udvikling. Det bør blandt andet dokumenteres:

- hvorfor de historiske personoplysninger er nødvendige,

- om formålet kan opnås med anonymiserede eller syntetiske data,
- om datamængden kan reduceres,
- hvor gamle oplysninger det er sagligt nødvendigt at anvende, og
- hvilke konkrete konsekvenser genanvendelsen kan have for de personer, oplysningerne vedrører.

4. Menneskelig kontrol skal kunne dokumenteres - ikke blot forudsættes

Det er positivt, at bemærkningerne i det nye lovforslag tydeligere beskriver, at menneskelig involvering i AI-baseret beslutningsstøtte skal være reel og meningsfuld og ikke må udgøre en tom gestus.

Men en rettighed, der ikke kan efterprøves, har begrænset værdi.

Der bør derfor indføres konkrete krav til sporbarhed.

Når AI anvendes som beslutningsstøtte i en sag med væsentlig betydning for en borger, bør myndigheden kunne dokumentere:

- hvilket output AI-systemet leverede,
- hvilke centrale faktorer systemet lagde vægt på,
- hvordan den menneskelige sagsbehandler vurderede outputtet,
- om sagsbehandleren afveg fra AI-systemets anbefaling, og
- hvem der traf den endelige beslutning.

Hvis dette ikke registreres, vil det efterfølgende kunne være meget vanskeligt for borgeren, tilsynsmyndigheder, klageorganer og domstole at afgøre, om den menneskelige kontrol reelt fandt sted.

Et generelt krav om dokumenterbar menneskelig kontrol bør derfor fremgå af selve loven.

Dette er særligt vigtigt, fordi lovbemærkningerne på side 19 udtrykkeligt anfører, at procedurer om identifikation af beslutningstager, dokumentation af afvigelser og relevant logning ganske vist kan understøtte kontrollen, men **ikke i sig selv er et krav efter loven**. Dermed risikerer en central retssikkerhedsgaranti at eksistere uden et tilsvarende obligatorisk bevisspor.

5. Bias og fejl kræver bindende minimumskrav

Lovforslaget erkender selv risikoen for, at historiske data kan indeholde skævheder, som et AI-system kan reproducere eller forstærke.

Dette er centralt.

Hvis historiske afgørelser, registreringer eller sagsmønstre allerede indeholder systematiske skævheder, kan et AI-system gøre disse langt mere effektive og langt vanskeligere at opdage.

Det foreliggende forslag opstiller imidlertid ikke fælles bindende minimumskrav til eksempelvis:

- validering,
- fejlrate,
- biasanalyse,
- test på relevante befolkningsgrupper,

- løbende overvågning,
- uafhængig revision, eller
- stopkriterier ved uacceptable resultater.

Dette bør ændres.

Det bør ikke alene være den enkelte myndighed eller systemejer, der definerer, hvornår et AI-system er "godt nok".

For systemer med væsentlig betydning for borgernes rettigheder bør der gælde fælles nationale minimumskrav til dokumenteret kvalitet og kontrol.

6. Borgerens rettigheder bør ikke tilpasses teknologiens begrænsninger

Lovforslagets § 4 giver mulighed for under nærmere betingelser at begrænse en række registreredes rettigheder efter databeskyttelsesforordningen.

Bemærkningerne beskriver blandt andet situationer, hvor indsigt eller sletning kan være vanskeligt eller teknisk problematisk, efter at personoplysninger er blevet integreret i et AI-system.

Dette rejser et grundlæggende spørgsmål:

> *Skal borgerens rettigheder tilpasses AI-systemets arkitektur, eller skal AI-systemets arkitektur tilpasses borgerens rettigheder?*

Udgangspunktet bør være det sidste.

Det bør fremgå klarere af loven, at en myndighed som hovedregel skal vælge eller udvikle systemer, der gør det muligt at efterleve gældende rettigheder.

At en bestemt teknisk løsning er vanskeligere, dyrere eller potentielt mindre præcis bør ikke i sig selv være tilstrækkeligt til at begrænse borgerens rettigheder.

I nogle situationer bør konsekvensen være, at det pågældende AI-system ikke må anvendes.

7. § 4 bør afgrænses direkte i loven

Det er ikke tilstrækkeligt alene at henvise til de overordnede krav i GDPR artikel 23.

Det bør fremgå direkte af loven:

- hvilke konkrete hensyn der kan begrunde begrænsning af borgernes rettigheder,
- hvilke rettigheder der kan begrænses,
- hvilke der ikke kan,
- hvor længe en begrænsning kan gælde,
- hvordan nødvendighed og proportionalitet skal dokumenteres, og
- hvilken kontrol der skal føres med anvendelsen.

En mulighed for at begrænse centrale databeskyttelsesrettigheder på hele sektorområder bør underlægges en meget høj tærskel og bør være genstand for offentlighed og ekstern kontrol.

8. Automatisk viderebehandling til AI-formål bør ikke blive en retlig genvej

Lovforslaget skal blandt andet fungere som nationalt retsgrundlag for viderebehandling af allerede indsamlede personoplysninger til udvikling af AI.

Dermed kan lovgiver på forhånd etablere et nyt retligt grundlag for en formålsændring, som ellers ville kræve en selvstændig vurdering.

Det er juridisk muligt inden for databeskyttelsesrettens rammer, men det gør lovens egne garantier desto vigtigere.

En generel hjemmel bør ikke få den praktiske effekt, at nødvendighed, dataminimering og borgerens rimelige forventninger reduceres til sekundære hensyn.

Der bør derfor indføres en eksplicit pligt til, før historiske eller allerede indsamlede personoplysninger anvendes til et nyt AI-formål, at dokumentere:

- nødvendigheden af den nye behandling,
- om formålet kan opnås på mindre indgribende måde,
- hvilke datakategorier der inddrages,
- hvilke persongrupper der påvirkes, og
- hvilke nye risici der opstår.

9. Der bør etableres et offentligt AI-register

For at sikre reel demokratisk kontrol bør borgere kunne se, hvor og hvordan staten anvender AI.

Jeg foreslår derfor et offentligt register over offentlige AI-systemer, som mindst angiver:

- myndigheden,
- systemets navn og leverandør,
- formålet,
- hvilke typer personoplysninger der anvendes,
- om følsomme personoplysninger indgår,
- om historiske sagsdata anvendes til træning,
- om profilering finder sted,
- hvilke afgørelser eller processer systemet understøtter,
- resultatet af risikovurderinger og relevante konsekvensanalyser,
- kendte fejl og begrænsninger, samt
- dato for seneste uafhængige kontrol.

Undtagelser kan naturligvis være nødvendige på særlige områder, eksempelvis af hensyn til national sikkerhed, men udgangspunktet bør være offentlighed.

10. Borgeren bør som udgangspunkt informeres om AI-anvendelse

Når et AI-system har haft en reel funktion i behandling af en borgers sag, bør borgeren som hovedregel have ret til at vide det.

Det bør ikke være nødvendigt først at opdage AI-anvendelsen gennem aktindsigt eller efter en klagesag.

Informationen bør være forståelig og omfatte systemets funktion, dets rolle i sagsbehandlingen og mulighederne for menneskelig prøvelse.

11. Følsomme data bør have en højere tærskel

Helbredsoplysninger, genetiske data og andre særligt beskyttede oplysninger bør ikke behandles på samme praktiske risikoniveau som almindelige administrative oplysninger.

Hvor sådanne data anvendes til AI-udvikling eller profilering, bør der gælde:

- skærpet nødvendighed,
- skærpet dataminimering,
- obligatorisk konsekvensanalyse,
- uafhængig kontrol,
- dokumenteret bias- og diskriminationstest, og
- som udgangspunkt forbud mod genbrug, hvor tilsvarende formål kan opnås med anonymiserede, syntetiske eller mindre indgribende data.

12. Parlamentarisk kontrol bør bevares ved særligt indgribende AI-anvendelser

En generel hjemmelslov bør ikke betyde, at alle fremtidige typer AI-anvendelse dermed på forhånd er politisk godkendt.

Visse anvendelser er så indgribende, at de bør kræve specifik lovgivning.

Det kan eksempelvis gælde AI-systemer, som anvender meget omfattende profilering eller følsomme oplysninger til vurderinger med væsentlige konsekvenser for den enkelte.

Her bør der være konkret demokratisk behandling af selve anvendelsen, ikke blot af den generelle infrastruktur omkring den.

13. Fejlagtig henvisning til GDPR artikel 13, stk. 4 bør rettes

På side 26 anføres det, at en myndighed eksempelvis kan være undtaget fra oplysningspligten, hvis videregivelse eller viderebehandling fremgår udtrykkeligt af lovgivningen, med henvisning til GDPR artikel 13, stk. 4, og artikel 14, stk. 5.

Dette er ikke korrekt for artikel 13, stk. 4. Denne bestemmelse vedrører alene den situation, hvor den registrerede allerede er bekendt med oplysningerne. Den lovbaserede undtagelse findes derimod i artikel 14, stk. 5, litra c, og vedrører den situation, hvor oplysningerne ikke er indsamlet hos den registrerede.

At der er tale om en reel intern fejl understøttes af, at lovudkastet på side 38 selv beskriver artikel 13, stk. 4, korrekt. Henvisningen på side 26 bør derfor rettes, så lovbemærkningerne ikke giver indtryk af en bredere undtagelse fra oplysningspligten, end GDPR faktisk hjemler.

14. Overgangsgab mellem den danske hjemmelslov og EU's højrisikokrav

Lovforslaget foreslås at træde i kraft dagen efter bekendtgørelse i Lovtidende. Samtidig er anvendelsestidspunktet for centrale krav til højrisiko-AI i EU's AI-forordning ændret i 2026.

For AI-systemer, der klassificeres som højrisiko efter artikel 6, stk. 2, og bilag III, finder kapitel III, afdeling 1-3, som udgangspunkt først anvendelse fra 2. december 2027. For visse produktbaserede højrisikosystemer efter artikel 6, stk. 1, og bilag I er datoen 2. august 2028.

Den danske lov kan dermed give et bredt nationalt behandlingsgrundlag i en periode, hvor flere af de EU-retlige højrisikoværn, som lovbemærkningerne ellers læner sig op ad - bl.a. risikostyring, dokumentation, logning, menneskeligt tilsyn og visse kvalitetskrav - endnu ikke finder fuld anvendelse.

Der bør derfor indføres overgangsbestemmelser eller nationale minimumskrav, som lukker dette beskyttelsesgab, indtil de relevante dele af AI-forordningen finder anvendelse.

15. Den tidligere artikel 9-konstruktion blev ændret markant - det taler for større lovmæssig forsigtighed

I den tidligere høringsrunde blev lovens AI-anvendelse koblet langt tættere til GDPR artikel 9, stk. 2, litra g, om væsentlige samfundsinteresser. I septemberudkastet præciseres derimod udtrykkeligt på side 30 og side 72, at brugen af AI i sig selv **ikke** udgør en væsentlig samfundsinteresse.

Det er en væsentlig juridisk korrektion af lovens begrundelse over tid. Det understreger efter min opfattelse behovet for, at de tilbageværende hjemler og garantier formuleres snævert og præcist i selve lovteksten, frem for at centrale retssikkerhedsspørgsmål overlades til efterfølgende sektorregulering og fortolkning.

16. Artikel 6, stk. 3 og kravet om klare og præcise nationale regler

Lovforslaget skal fungere som et meget bredt supplerende nationalt retsgrundlag efter GDPR artikel 6, stk. 3. EU-Domstolen har gentagne gange fremhævet, at lovgivning, der griber ind i retten til databeskyttelse, skal indeholde klare og præcise regler om indgrebets rækkevidde og anvendelse samt minimumsgarantier mod misbrug og ulovlig adgang.

Dette rejser et grundlæggende spørgsmål om proportionaliteten i en generel hjemmel, der kan omfatte meget forskellige områder som socialforvaltning, sundhedsnære administrative funktioner, skat, forsyning, domstole og andre offentlige opgaver.

Det bør derfor fremgå langt tydeligere af loven, hvilke kategorier af behandlinger, datatyper, registrerede, anvendelsesformål og sikkerhedsforanstaltninger der kan omfattes, særligt hvor AI-profilering eller beslutningsstøtte kan få væsentlig betydning for den enkelte.

17. Interne databehandlingspolitikker bør ikke sammenblandes med det retlige garantiniveau

På side 31 nævnes det, at beskyttelsesforanstaltninger allerede kan følge af blandt andet sektorlovgivning eller individuelle dataansvarliges databehandlingspolitikker.

Interne tekniske og organisatoriske politikker er naturligvis relevante for efterlevelsen af GDPR. Men hvor en behandling af særlige kategorier af personoplysninger beror på eksempelvis artikel 9, stk. 2, litra g, stiller GDPR selv krav om et retligt grundlag, der er proportionelt og sikrer passende og specifikke foranstaltninger.

Lovbemærkningerne bør derfor skelne skarpere mellem de **retlige garantier**, som skal følge af lovgivningen, og den dataansvarliges **interne implementering** af disse garantier.

18. Princip 7 om forebyggelse af snyd og fejl kan ikke uden videre erklæres irrelevant

På side 50 vurderes princip 7 for digitaliseringsklar lovgivning om forebyggelse af snyd og fejl som ikke relevant for lovforslaget.

Det forekommer vanskeligt at forene med lovens eget indhold. Lovforslaget regulerer netop AI-baseret profilering, beslutningsstøtte, genanvendelse af historiske data og delvis automatisering. Lovbemærkningerne behandler selv risikoen for bias og fejl.

Digitaliseringsstyrelsens egen vejledning til princip 7 angiver, at der allerede ved lovgivningens udformning bør tages højde for efterfølgende kontrol og forebyggelse af fejl. Folketingets Ombudsmand fremhæver samtidig, at forvaltningsretlige krav skal indtænkes i offentlige it-systemer fra starten, herunder krav om dokumentation og journalisering.

Vurderingen af princip 7 bør derfor genforetages og begrundes konkret.

19. Lovforslaget kan på længere sigt erstatte mere specifikke sektorhjemler

På side 15-16 fremgår det, at eksisterende sektorlovgivning fortsat kan gælde sideløbende med lovforslaget. Det anføres imidlertid også, at det ved senere revision af sektorlovgivningen kan overvejes, om AI-behandling i stedet bør ske med hjemmel i den generelle AI-hjemmelslov.

Dermed kan loven over tid udvikle sig fra et supplerende fælles grundlag til en mere generel opsamlingshjemmel, som afløser sektorspecifikke løsninger.

Det gør det særligt vigtigt, at loven fra begyndelsen indeholder et højt fælles minimumsniveau af retssikkerhed. Jeg foreslår derfor en lovbestemt evaluering efter senest tre år og på ny efter fuld anvendelse af AI-forordningens højrisikoregler, samt krav om at Folketinget orienteres om, hvilke sektorhjemler der er blevet erstattet eller udfaset til fordel for denne lov.

20. Høringsprocessen bør sikre, at de aktører, som nu direkte berøres af udvidelsen, høres igen

Forsyningsorganisationerne DANVA, Cirkulær, Dansk Fjernvarme og Danske Vandværker afgav i den tidligere høringsrunde et fælles svar, hvor de pegede på, at deres sektorer faldt uden for den daværende generelle AI-hjemmel. Septemberudkastet udvider anvendelsesområdet på en måde, som bl.a. kan omfatte kommunalt ejede forsyningsselskaber.

De nævnte organisationer fremgår imidlertid ikke af den nye høringsliste, samtidig med at høringsbrevet oplyser, at tidligere høringssvar ikke automatisk offentliggøres i den nye høringsrunde, medmindre de genfremsendes.

Når lovforslaget er ændret i en retning, der gør deres sektor direkte relevant, bør det sikres, at disse aktører faktisk får mulighed for at forholde sig til den nye konstruktion og dens retssikkerhedsmæssige følgevirkninger.

21. Konkrete lovtekniske ændringer, der bør overvejes før fremsættelse

De ovenstående indsigelser kan efter min opfattelse omsættes til forholdsvis præcise ændringer i lovforslaget. Formålet er ikke at begrænse enhver offentlig anvendelse af AI, men at sikre, at den brede generelle hjemmel ledsages af et tilsvarende tydeligt fælles sikkerhedsniveau.

§ 3, stk. 2 - bindende minimumsværn. Bestemmelsen bør som minimum fastslå, at der ved behandling af oplysninger omfattet af GDPR artikel 9 eller 10 skal være passende og specifikke foranstaltninger på plads, før behandlingen påbegyndes. En mulig lovteknisk model kunne være:

> "*Ved behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9 eller artikel 10 skal der fastsættes passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Foranstaltningerne skal være fastlagt, før behandlingen påbegyndes.*"

Dokumentation af menneskelig kontrol. Når AI anvendes som beslutningsstøtte i en sag med væsentlig betydning for den registrerede, bør myndigheden kunne dokumentere systemets relevante output, den ansvarlige menneskelige beslutningstager og den endelige selvstændige vurdering. Dokumentationen bør være tilstrækkelig til efterfølgende kontrol, klage og domstolsprøvelse.

§ 4 - nødvendighed og proportionalitet direkte i lovteksten. Det bør fremgå udtrykkeligt, at en begrænsning af registreredes rettigheder kun kan ske, når den er nødvendig, proportional, konkret begrundet og tidsmæssigt afgrænset. Det bør samtidig præciseres, at teknisk bekvemmelighed, administrative omkostninger eller AI-systemets præcision ikke i sig selv er tilstrækkelig begrundelse.

Overgangsværn. Der bør indsættes en overgangsregel, som sikrer nationale minimumskrav til de relevante højrisikoanvendelser i perioden fra lovens ikrafttræden og frem til de tilsvarende bindende krav i AI-forordningen finder anvendelse.

Lovbestemt evaluering. Loven bør evalueres senest tre år efter ikrafttrædelsen og igen efter fuld anvendelse af de relevante højrisikoregler i AI-forordningen. Evalueringen bør forelægges Folketinget og som minimum redegøre for anvendelsen af § 3 og § 4, berørte datakategorier, dokumenterede fejl og hændelser samt eventuelle sektorspecifikke hjemler, der er blevet erstattet af den generelle lov.

Afsluttende bemærkning

AI kan uden tvivl give betydelige gevinster i den offentlige sektor.

Men netop fordi teknologien kan analysere meget store datamængder, identificere mønstre, profilere borgere og påvirke beslutninger i en skala, som traditionel manuel sagsbehandling aldrig har kunnet, bør retssikkerheden styrkes tilsvarende.

Det afgørende spørgsmål er derfor ikke, om det offentlige skal kunne anvende AI.

Det afgørende spørgsmål er, hvilke rettigheder borgeren skal have, når det offentlige gør det.

Efter min vurdering bør lovforslaget derfor ændres, således at:

- der indføres fælles bindende minimumsgarantier for følsomme personoplysninger,
- "kan" i § 3, stk. 2, erstattes af en bindende pligt i relevante tilfælde,
- menneskelig kontrol bliver dokumenterbar og efterprøvbar,
- der indføres bindende kvalitets-, bias- og kontrolkrav,
- § 4 indsnævres og præciseres direkte i lovteksten,
- borgerrettigheder som udgangspunkt skal styre systemdesignet og ikke omvendt,
- historiske data underlægges en særskilt nødvendigheds- og proportionalitetsvurdering, og

- der etableres reel offentlig gennemsigtighed omkring myndighedernes AI-systemer,
- den interne modstrid mellem "kan" og "skal" ved særlige beskyttelsesforanstaltninger rettes,
- den fejlagtige henvisning til GDPR artikel 13, stk. 4, korrigeres,
- der etableres nationale overgangsværn frem til AI-forordningens højrisikokrav finder fuld anvendelse,
- vurderingen af princip 7 om forebyggelse af snyd og fejl genforetages, og
- loven underlægges en fast evaluering, så en gradvis erstatning af sektorspecifikke hjemler kan kontrolleres demokratisk.

En bred generel AI-hjemmel bør ledsages af brede generelle rettigheder.

Ellers risikerer lovforslaget at skabe en permanent asymmetri: myndighedernes teknologiske handlemuligheder bliver meget konkrete, mens borgernes beskyttelse i for høj grad bliver afhængig af efterfølgende fortolkninger, sektorregler og administrative vurderinger.

Kilder og centrale henvisninger

- Udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger, høring nr. 71477, særligt s. 15-16, 19, 26, 30-32, 38, 46 og 50.
- Europa-Parlamentets og Rådets forordning (EU) 2016/679 (GDPR), særligt artikel 6, 9, 13, 14, 23 og 25.
- Forordning (EU) 2026/1744 om ændret anvendelsestidspunkt for dele af AI-forordningens højrisikoregler.
- EU-Domstolen, ECLI:EU:C:2026:496, navnlig præmis 72-73 om klare og præcise regler og minimumsgarantier.
- Digitaliseringsstyrelsen: Vejledning om digitaliseringsklar lovgivning, princip 7 - forebyggelse af snyd og fejl.
- Folketingets Ombudsmand: Generelle forvaltningsretlige krav til offentlige it-systemer.
- Dataetisk Råds høringssvar til den tidligere version af lovforslaget.
- DANVA, Cirkulær, Dansk Fjernvarme og Danske Vandværker: fælles høringssvar af 5. marts 2026.

Med venlig hilsen

Johnny Rivli

Høringssvar om AI-hjemmelsloven

12. oktober 2026

Til: Digitaliseringsstyrelsen
Fra: Morten Larsen, privatperson
Vedrørende: Forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger
Høringsgrundlag: Det reviderede lovforslag af 14. september 2026. Høringsfrist 12. oktober 2026 kl. 12. [1]

1. Indledning og samlet vurdering

Jeg afgiver dette høringssvar som privatperson på eget initiativ. Jeg støtter ikke en generel adgang til at bruge borgernes personoplysninger til udvikling og anvendelse af AI i den offentlige sektor. Mit krav er fuld anonymitet. Hvis oplysningerne eller resultaterne kan føres tilbage til den enkelte borger, er jeg imod, at de bruges på denne måde.

Oplysninger, som borgerne har afgivet til en myndighed, bør ikke blive et generelt råstof for nye analyser, profilering og beslutningsstøtte. En ny lovhjemmel - altså en juridisk tilladelse - gør ikke i sig selv behandlingen forsvarlig. Den ændrer heller ikke behovet for at beskytte borgerne efter databeskyttelsesforordningen, GDPR.

Nedenfor gennemgår jeg lovforslagets vigtigste bestemmelser, forskning om genidentifikation og konkrete myndighedsdokumenter fra beskæftigelsesområdet, Statens Serum Institut og den offentlige brug af Microsoft Copilot. For hvert eksempel beskriver jeg, hvad materialet viser, og hvorfor det har betydning for lovforslaget. Kilderne er identificeret til sidst.

Hvis lovgiver alligevel viderefører ordningen, bør følgende som minimum sikres:

1. Dokumentation før brug: Myndigheden skal kunne redegøre for formål, data, lovlig opbevaring, ansvar og gennemførte beskyttelsesforanstaltninger, før behandlingen begynder.
2. Klare grænser for nye formål: Oplysninger indsamlet til én myndighedsopgave må ikke uden en tilstrækkelig begrundelse åbnes for andre anvendelser.
3. Borgernes rettigheder og reel kontrol: Beskyttelsen skal være bindende og kunne gennemføres i praksis. En medarbejders formelle godkendelse af et AI-resultat er ikke nok.
4. Placeret ansvar og offentlighed: Det skal være tydeligt, hvem der har ansvaret, hvilke systemer der bruges, og hvordan fejl, ændringer og ophør håndteres.

Mine konkrete anbefalinger skal beskytte borgerne, hvis ordningen videreføres. De er ikke en tilslutning til lovforslaget og fjerner ikke min grundlæggende indvending mod AI-behandling af oplysninger, der kan knyttes til mennesker.

2. Hvad lovforslaget lægger op til

Høringen vedrører det reviderede lovforslag af 14. september 2026. Forslaget skal give offentlige myndigheder en generel hjemmel til at udvikle og bruge AI som led i deres lovbestemte opgaver, blandt andet til profilering og beslutningsstøtte. Profilering vil her sige, at oplysninger bruges til at vurdere eller forudsige forhold ved en borger. [1]

Lovforslagets bemærkninger indeholder følgende afgrænsninger:

- § 1 knytter ordningen til behandling efter artikel 6, stk. 1, litra e, inden for myndighedernes lovbestemte opgaver.
- GDPR og anden relevant lovgivning gælder fortsat. Der skal udarbejdes en konsekvensanalyse - en systematisk vurdering af risiciene for borgernes rettigheder - når artikel 35 kræver det.

- § 3 skal ikke i sig selv give adgang til at indsamle yderligere oplysninger eller udveksle oplysninger frit mellem myndigheder.
- Oplysninger, der burde være slettet, må ikke bruges til AI, blot fordi en kopi stadig findes. Mulig fremtidig AI-udvikling skal heller ikke begrunde forlænget opbevaring.
- Lovforslaget giver efter bemærkningerne ikke hjemmel til fuldautomatiske afgørelser efter artikel 22. § 4 begrænser ikke selv rettigheder og omfatter ikke direkte artikel 13 og 14. [1, s. 7-10, 28-34, 42-43 og 68-79]

Disse afgrænsninger bør omsættes til bindende betingelser, som kan kontrolleres før behandlingsstart. Henvisninger til efterfølgende vurderinger, interne politikker og eventuelle bekendtgørelser giver efter min vurdering ikke tilstrækkelig klarhed.

Datatilsynets høringssvar af 3. marts 2026 bruges nedenfor som dokumentation for tilsynets tidligere bemærkninger. Det vedrører forslaget fra februar og skal holdes adskilt fra tilsynets nye udmelding omtalt nedenfor. [3]

Datatilsynet har i sin nyhed af 12. oktober 2026 oplyst, at det har afgivet et nyt høringssvar. Tilsynet anerkender ændringerne i lovforslaget, men understreger, at en hjemmel ikke alene løser databeskyttelsesspørgsmålene. Krav om sikkerhed, rettigheder, tredjelandsoverførsler og ændrede behandlingsformål skal være afklaret før behandlingsstart. Selve det nye høringssvar er endnu ikke offentliggjort; henvisningen her gælder derfor nyheden. [15]

Udmeldingen understøtter efter min vurdering kravet om afklaring før behandlingsstart. Den besvarer ikke i sig selv mine indsigelser mod lovforslaget eller mit krav om fuld anonymitet.

3. Fuld anonymitet skal være en forudsætning

Med fuld anonymitet mener jeg, at oplysningerne og AI-systemets resultater ikke kan knyttes til en bestemt borger, heller ikke ved sammenstilling med andre oplysninger. Fjernelse af navn og CPR-nummer er ikke nok, hvis eksempelvis hændelser, helbredsforhold, arbejdsforløb eller andre kendetegn kan afsløre personen. Hvis fuld anonymitet ikke kan sikres, er jeg imod anvendelsen. Det er mit krav til den ordning, jeg vil kunne støtte.

Pseudonymisering betyder, at oplysningerne behandles, så de ikke kan henføres til en bestemt person uden yderligere oplysninger, for eksempel en særskilt nøgle. Det kan være en beskyttelse, men er ikke i sig selv dokumentation for anonymitet. GDPR's betragtning 26 kræver en konkret vurdering af mulighederne for identifikation, blandt andet med hensyn til tid, omkostninger, tilgængelig teknologi og teknologiens udvikling. [2, artikel 4 og betragtning 26]

Den juridiske vurdering er således ikke en ubetinget garanti mod enhver tænkelig fremtidig genidentifikation. Mit krav om fuld anonymitet er mit standpunkt til lovforslaget. Jeg ønsker ikke, at usikkerhed om beskyttelsen bliver et argument for at lade borgerne bære risikoen.

Forskningen viser, hvorfor det ikke er tilstrækkeligt blot at fjerne direkte identifikatorer. Robin Staab og medforfattere viser i et studie fra ICLR 2024, at sprogmodeller kan udlede personlige egenskaber fra tekst på Reddit, og at almindelig tekstmaskering ikke nødvendigvis hindrer dette. Det handler om at udlede oplysninger om personen og er ikke det samme som at finde personens navn. [13]

Jianing Wen og Tianshi Li undersøger i AgentDoxx fra 4. oktober 2026, hvordan sprogmodeller med websøgning kan forbinde anonymiserede interviewtekster med navngivne personer. Undersøgelsen er et preprint og bygger på syntetiske interviews baseret på offentlige oplysninger om personer med kendte identiteter. Den giver derfor ikke en generel genidentifikationsrate for danske myndighedsregistre. [14]

Studierne dokumenterer konkrete risici ved udledning og genidentifikation. De beviser ikke, at enhver anonymisering kan brydes. De understøtter mit krav om, at myndighederne skal forklare og efterprøve beskyttelsen i den konkrete løsning, herunder med relevante eksterne oplysninger og realistiske adgangsmuligheder. En betegnelse som anonymiseret eller pseudonymiseret kan ikke stå alene.

Brug af oplysninger, der allerede er reelt anonyme, falder som udgangspunkt uden for GDPR. Selve arbejdet med at anonymisere personoplysninger er derimod fortsat en behandling, som skal have et lovligt grundlag. Jeg beder derfor lovgiver prioritere løsninger, hvor borgerne ikke kan identificeres i den efterfølgende AI-behandling, frem for at skabe en bred adgang til personhenførbare data. [2, artikel 4 og betragtning 26]

4. Historiske data og nye formål (§ 3)

4.1 Lovgiver skal begrunde den brede adgang

På s. 34 og 70-71 forklares, at loven skal udgøre grundlag for viderebehandling efter artikel 6, stk. 4, så myndighederne ikke skal foretage den almindelige konkrete vurdering af, om det nye formål er foreneligt med det oprindelige. Det omfatter både historiske og lukkede sager og oplysninger fra aktive sager. [1]

Artikel 6, stk. 4, stiller krav til en national lov, som skal give adgang til at bruge oplysninger til andre formål. Loven skal være nødvendig og forholdsmæssig og bygge på et af de hensyn, der er nævnt i artikel 23, stk. 1. En generel henvisning til national ret besvarer ikke, hvorfor netop denne brede adgang er nødvendig. [2]

Datatilsynet efterlyste i marts netop en forklaring på, hvilke hensyn der kunne begrunde så omfattende viderebehandling. Lovforslaget præciserer bl.a. lovlig opbevaring og afgrænsningen over for videregivelse. Jeg savner fortsat en tilstrækkelig konkret begrundelse for, at den generelle adgang på tværs af meget forskellige myndighedsopgaver opfylder artikel 6, stk. 4. [1, s. 33-35 og 70-72; 3, s. 10-13]

Jeg beder derfor ministeriet redegøre særskilt for, hvilke mål efter artikel 23, stk. 1, der bærer hvilke former for viderebehandling, hvilke indgreb der er nødvendige, og hvilke mindre indgribende muligheder der er vurderet. Indgribende profilering af borgere bør afgrænses efter behandlingsformål, datakategorier, personkreds og konsekvenser. Hvor den generelle lov ikke kan give tilstrækkelig klarhed, bør der kræves et mere præcist retsgrundlag for den pågældende behandling.

4.2 Oplysningerne skal være lovligt opbevaret

Bemærkningernes afgrænsning af historiske oplysninger er væsentlig, men bør omsættes til en bindende adgangsbetingelse. Før oplysninger indgår i udvikling, træning, test, validering, gentræning eller drift, bør myndigheden dokumentere:

- hvilke datasæt og kopier der indgår, hvorfra de stammer, og hvilket formål de oprindeligt blev indsamlet til;
- grundlaget for fortsat opbevaring, den gældende slettefrist, dens startpunkt og eventuelle lovlige undtagelser;
- hvorfor oplysningerne er nødvendige og egnede til det konkrete AI-formål, herunder deres kvalitet, alder og kendte fejl;
- hvordan senere berigtigelser, sletning og begrænsning håndteres i de nye behandlingsled;
- hvilke særlige formålsbindinger der fortsat gælder, eksempelvis for oplysninger indsamlet til forskning og statistik.

Uafklaret slette- eller hjemmelsstatus bør føre til, at de berørte oplysninger holdes uden for den nye AI-behandling, indtil forholdet er afklaret. Kravet kan opfyldes gennem velafgrænsede datasæt og kontroller; det behøver ikke bestå i en manuel juridisk vurdering af hvert enkelt datafelt hos hver borger.

4.3 Eksempel: slettefrister på beskæftigelsesområdet

Styrelsen for Arbejdsmarked og Rekruttering (STAR) oplyste den 4. september 2026, at slettefristen for styrelsens statistiske datavarehus, betegnet DSDW, var præciseret til 35 år fra etableringen i 2008. Den samtidig udleverede slettepolitik DOA-1A angiver derimod 35 år fra 12. juni 2009 og første sletning 12. juni 2044. Politikken var godkendt 12. januar 2026. Der er dermed en konkret forskel i dokumenternes angivelse af, hvornår fristen begynder. [7, s. 9; 8, s. 3]

Politikken beskriver også, at hovedfristens slettemekanisme skal fastlægges før fristens udløb, og at kontrollen endnu ikke var fastsat. Den oplyser samtidig, at der sker løbende sletning i driftsrutiner. Materialet dokumenterer således en uoverensstemmelse om fristens begyndelse og et behov for nærmere afklaring af kontrollen; det dokumenterer ikke, at STAR aldrig sletter, eller at en bestemt opbevaringsperiode allerede er kendt ulovlig.

STAR oplyste efterfølgende den 30. september 2026, at automatisk sletning er implementeret for alle dataområder i Det Fælles Datagrundlag (DFDG). Det er et andet system end det statistiske datavarehus, som eksemplet ovenfor vedrører. Den nye oplysning skal derfor med i billedet, men afklarer ikke i sig selv forskellen mellem de to angivelser af datavarehusets slettefrist. [12, s. 6]

For lovforslaget er pointen konkret: En myndighed skal kunne give ét sammenhængende svar på den gældende opbevaringsregel og dens gennemførelse, før oplysningerne bruges i et nyt AI-forløb.

5. Beskyttelsen skal være bindende (§ 3, stk. 2)

Lovforslaget præciserer, at AI i sig selv ikke udgør en væsentlig samfundsinteresse efter artikel 9, stk. 2, litra g, og at de nødvendige garantier skal foreligge før behandlingen. Det er en vigtig præmis. Samtidig åbner bemærkningerne på s. 31 og 73 for, at individuelle dataansvarliges databehandlingspolitikker kan indgå i vurderingen af, at yderligere regler ikke er nødvendige. [1]

Her bør loven og bemærkningerne skelne klart mellem det retligt nødvendige grundlag og den praktiske gennemførelse. Interne politikker kan være relevante organisatoriske foranstaltninger. De kan ikke i sig selv erstatte de garantier, som efter den anvendte bestemmelse skal være sikret ved lovgivning. Ministeriet bør præcisere, hvilke krav der skal følge af lov eller bekendtgørelse, hvilke der kan konkretiseres internt, og hvordan deres gennemførelse efterprøves. [2, artikel 9, stk. 2, litra g]

Bemærkningerne bør desuden bringes i klar indbyrdes sammenhæng. S. 30 og 72 kræver et eksisterende relevant grundlag efter artikel 9 og understreger, at AI ikke i sig selv er en væsentlig samfundsinteresse. S. 44 begrunder derimod mere generelt et supplerende grundlag, også efter artikel 9, med kvalitet og effektivitet. Det bør fremgå entydigt, hvad § 3 tilfører, og hvilke konkrete betingelser der fortsat skal være opfyldt for hver behandling.

Beskyttelsen bør også omfatte indgribende behandling af oplysninger, som ikke hører under GDPR's særlige regler om følsomme oplysninger i artikel 9 eller strafbare forhold i artikel 10. Profilering med andre oplysninger kan få stor betydning for en borgers forsørgelse, uddannelse eller adgang til hjælp. Datatilsynet fremhævede dette i marts, og lovforslaget omtaler selv sårbare personer og udledte følsomme oplysninger. [3, s. 9-10; 1, s. 32 og 74]

Jeg foreslår derfor en fælles bindende minimumsbeskyttelse for indgribende anvendelser, suppleret med sektorspecifikke regler. Den bør omfatte børn og sårbare borgere, datakvalitet og skævheder, nødvendige datakilder, adgang, rettigheder, kontrol og ophør. Det bør være dokumenteret før start, hvorfor eksisterende garantier er tilstrækkelige, eller hvilke yderligere regler og foranstaltninger der skal gennemføres.

6. Privatlivsbeskyttelse skal indbygges fra begyndelsen

GDPR's artikel 25 handler om databeskyttelse gennem design og standardindstillinger. Beskyttelsen skal altså indbygges i systemet og være udgangspunktet for dets brug. Det Europæiske Databeskyttelsesråd (EDPB) fremhæver, at foranstaltningerne skal virke i praksis og vurderes gennem behandlingens levetid, også i eksisterende systemer. Dette bør fremgå tydeligt af betingelserne for at bruge den nye hjemmel. [1, s. 29; 2; 4]

Hvis behandling med personoplysninger videreføres, bør myndigheden som minimum dokumentere følgende:

1. Hvilke oplysninger systemet har adgang til, og hvilke der faktisk bruges til den enkelte opgave.
2. Hvorfor opgaven ikke kan løses med reelt anonyme oplysninger, færre data, kortere historik eller en anden indretning af systemet.
3. Hvordan uvedkommende, forældede og sletningsmodne oplysninger holdes ude, og hvordan fejl og bestridte oplysninger håndteres.
4. Hvordan borgerens ret til indsigt, berigtigelse, sletning og begrænsning gennemføres, når betingelserne for rettigheden er opfyldt.
5. Hvilke beskyttelser der er gennemført og afprøvet, og hvem der følger op, når systemet ændres.

Disse minimumskrav er ikke en erstatning for mit krav om anonymitet. De skal gøre myndighedens valg og den faktiske beskyttelse efterprøvelige, hvis lovgiver viderefører behandling med personoplysninger.

En medarbejders eksisterende adgang til et stort dokumentområde viser heller ikke i sig selv, at automatisk søgning og sammenstilling af alle tilgængelige oplysninger er nødvendig for enhver opgave. Den konkrete behandling skal afgrænses efter formålet, også når de tekniske adgangsrettigheder respekteres.

Vurderingen skal følge oplysningerne gennem hele systemet: fra det oprindelige register til træningskopier, søgeindeks, brugerens instruktioner til AI-systemet, svar og historik. Sletning i det oprindelige register fjerner ikke nødvendigvis oplysninger andre steder. Det skal også vurderes, om selve den trænede model kan afsløre personoplysninger. EDPB's udtalelse 28/2024 behandler betingelserne for at anse en AI-model for anonym. [6]

Eksempler: Microsoft Copilot og Statens Serum Institut

Microsoft Copilot for Microsoft 365 er en AI-assistent til blandt andet arbejde med dokumenter. Den fælles offentlige konsekvensanalyse, version 2.0 af 23. februar 2026, kræver, at de beskrevne foranstaltninger gennemføres før behandling. Databeskyttelsesrådgiveren, også kaldet DPO'en, understreger, at denne fælles analyse ikke i sig selv dokumenterer lovlighed hos den enkelte myndighed. Myndigheden skal tage stilling til sin egen anvendelse og sine lokale risici. Rådgiveren peger også på risikoen for utilstrækkelig menneskelig kontrol. [9, s. 225-229]

Dette dokumenterer betingelser i analysen. Det dokumenterer ikke, om en bestemt myndighed har eller ikke har gennemført dem. Netop derfor bør loven kræve lokal dokumentation for, at betingelserne er opfyldt.

Statens Serum Institut (SSI) oplyste i en aktindsigtsafgørelse af 24. september 2026, at et internt notat og den særskilte konsekvensanalyse for forskningsprojektet Bedre sundhed i generationer (BSIG) fortsat var foreløbige. Instituttet beskrev et igangværende arbejde med at afklare databeskyttelsesforhold og planlægge korrigerende handlinger. Beskrivelserne og vurderingerne var endnu ikke endeligt kvalitetssikrede. [10, s. 6-7]

Eksemplet viser et konkret tilfælde, hvor en myndighed selv beskriver sin dokumentation som uafsluttet. Det er ikke en afgørelse om en ulovlig AI-anvendelse. Relevansen for lovforslaget er, at adgang til nye formål ikke bør bygge på en antagelse om, at eksisterende dokumentation allerede dækker dem.

7. Rettigheder må ikke vige for den valgte teknik (§ 4)

§ 4 giver mulighed for senere at begrænse rettigheder efter artikel 12 og 15-21 inden for artikel 23. Bemærkningerne anerkender nødvendighed og proportionalitet, men begrunder også ordningen med vanskeligheder ved at udskille oplysninger fra modelparametre og med hensynet til systemets præcision. Der åbnes både for regler om bestemte systemer og om hele sektorområder. [1, s. 40-46 og 76-79]

Det skaber efter min vurdering et centralt spørgsmål om rækkefølgen: Hvis myndigheden først vælger en arkitektur, hvor rettighederne er vanskelige at opfylde, og derefter bruger vanskeligheden som argument for at begrænse dem, risikerer den valgte teknik at udhule artikel 25.

En teknisk vanskelighed eller en økonomisk omkostning er ikke i sig selv tilstrækkelig begrundelse for en begrænsning efter artikel 23. Det beskyttede samfundshensyn, nødvendigheden og proportionaliteten skal identificeres. EDPB's retningslinjer 10/2020 og Datatilsynets tidligere høringssvar understøtter kravet om en konkret og forudsigelig afgrænsning. [2; 3, s. 13-15; 5]

Jeg anbefaler, at § 4 udtrykkeligt kræver:

- angivelse af den berørte rettighed, behandling, personkreds og det konkrete hensyn efter artikel 23, stk. 1;
- en dokumenteret vurdering af nødvendighed, proportionalitet og mindre indgribende løsninger, herunder andre designvalg efter artikel 25;
- at begrænsningen alene rammer de dele af rettigheden og behandlingen, hvor den er nødvendig;
- fastlagt varighed eller revisionstidspunkt og de relevante garantier efter artikel 23, stk. 2;
- klar information om begrænsningen og praktisk adgang til klage og prøvelse, under hensyn til lovlige undtagelser fra information;
- offentliggørelse af et begrundet grundlag for bekendtgørelsen i en form, der beskytter fortrolige oplysninger og sikkerhed.

En vanskelighed ved modelparametre bør eksempelvis ikke automatisk begrænse adgangen til oplysninger i et særskilt træningsdatasæt, et søgeindeks eller en log, hvor rettigheden kan gennemføres. Ligeledes bør generelle henvisninger til en sektor ikke erstatte vurderingen af de konkrete behandlinger.

Jeg foreslår en udtrykkelig regel om, at systemets tekniske indretning, præcision eller omkostningerne ved rettighedsopfyldelse ikke alene kan begrunde en begrænsning. En leverandøraftale eller produktbeslutning skal heller ikke i praksis foregribe den retlige vurdering.

Det bør samtidig præciseres, hvordan en begrænsning af artikel 12 afgrænses, så oplysningspligterne i artikel 13 og 14 fortsat kan opfyldes. Bemærkningernes fælles omtale af artikel 13, stk. 4, og artikel 14, stk. 5, bør skelne tydeligere mellem deres forskellige undtagelser. Artikel 13, stk. 4, indeholder ikke den generelle undtagelse om uforholdsmæssig indsats, der findes i artikel 14, stk. 5, litra b. [1, s. 43 og 79; 2]

8. Menneskelig kontrol skal være reel

Lovforslagets bemærkninger siger, at en menneskelig godkendelse ikke må være en formalitet. Samtidig beskrives procedurer om beslutningskompetence, afvigelser og logning som noget, loven ikke i sig selv kræver. Den forskel bør fjernes: Hvis menneskelig kontrol skal beskytte borgeren, skal den kunne påvises i den konkrete behandling. [1, s. 18-19 og 63-65]

GDPR's artikel 22 og betragtning 71 er relevante, når en afgørelse reelt træffes alene ved automatisk behandling og har retsvirkning eller tilsvarende væsentlig betydning for borgeren. Betragtning 71 fremhæver blandt andet menneskelig indgriben, mulighed for at fremføre sit synspunkt og mulighed for at anfægte afgørelsen. Det afgørende er den faktiske beslutningsproces. Betegnelsen beslutningsstøtte gør ikke en rent formel menneskelig godkendelse til en selvstændig vurdering. [2]

Jeg foreslår, at loven gør det bindende at kunne dokumentere den reelle kontrol ved beslutningsstøtte med væsentlig betydning for borgeren. Dokumentationen bør stå i forhold til risikoen og vise, at den ansvarlige person har:

- kompetence, tid og adgang til de relevante kilder;
- mulighed og mandat til at afvise eller ændre systemets forslag;
- kendskab til systemets begrænsninger og til usikkerhed i det konkrete output;
- pligt til at foretage en selvstændig vurdering, som kan efterprøves efterfølgende.

Logning betyder registrering af, hvad der er sket i systemet. Myndigheden bør kunne vise, hvordan AI indgik i en væsentlig beslutning, men dokumentationen skal selv begrænses til det nødvendige og have klare adgangs- og slettefrister. Det er ikke et krav om at gemme alle oplysninger og alle instruktioner til systemet.

Den irske Data Protection Commissions rapport, offentliggjort 24. september 2026, beskriver et eksempel, hvor menneskelig aktivering og efterfølgende klageadgang ikke i sig selv var tilstrækkeligt. Processen blev ændret, så menneskelig involvering fandt sted før den indgribende beslutning. Rapporten fremhæver også konkret dokumentation og særlig opmærksomhed ved historiske data. [11, s. 37-40, 49-50 og 59]

Det er relevante tilsynserfaringer, ikke bindende dansk praksis eller en generel godkendelse af AI. Rapportens behandling af private virksomheders interesseafvejning efter artikel 6, stk. 1, litra f, kan heller ikke overføres direkte til myndigheders opgaver efter litra e.

Grænsen til artikel 22 bør desuden stå direkte i § 3: Bestemmelsen giver ikke i sig selv hjemmel til afgørelser omfattet af artikel 22, stk. 1.

9. Ansvar, leverandører og offentlig kontrol

Et behandlingsforløb kan involvere kilderegistre, en fælles offentlig platform, en privat modelleverandør, underdatabehandlere og den myndighed, som bruger resultatet. Der bør foreligge én sammenhængende beskrivelse af forløbet, hvor ansvaret for hver behandling og kontrol er placeret. Det ændrer ikke GDPR's konkrete fordeling af dataansvar og databehandleransvar. [2, artikel 24, 26 og 28]

Den ansvarlige ledelse bør før start dokumentere sin beslutning på grundlag af risikovurderingen og, når reglerne kræver det, en ajourført konsekvensanalyse. Databeskyttelsesrådgiveren skal inddrages som rådgiver. Ansvaret for behandlingen skal fortsat ligge hos den ansvarlige myndighed.

Vurderingen bør omfatte hele den faktiske leverandørkæde, herunder relevante integrationer, supportadgang, model- og produktændringer, opbevaring og eventuelle tredjelandsoverførsler. Den skal omfatte risikoen for sammenstilling, udledning af nye oplysninger og misbrug af brede adgange. Der skal være mulighed for at standse behandlingen, hvis forudsætningerne ikke længere holder. Forudgående høring efter artikel 36 skal ske, når betingelserne er opfyldt. [2]

Jeg foreslår desuden en offentlig oversigt over behandlinger, som støttes på loven, med formål, ansvarlig myndighed, datakategorier, borgergrupper, status og eventuelle rettighedsbegrænsninger. Et forståeligt resumé af risikovurdering og beskyttelsesforanstaltninger bør offentliggøres, med konkret beskyttelse af personoplysninger og oplysninger, hvis offentliggørelse ville skade sikkerheden.

Den foreslåede oversigt bør samordnes med registreringsordningen i EU's AI-forordning, herunder artikel 49 og 71. Artikel 71 vedrører en EU-database for bestemte AI-systemer. Jeg efterspørger et forståeligt overblik over alle offentlige anvendelser, der støttes på den danske lov, også hvor EU's registreringsordning ikke giver et offentligt overblik. Registrering dokumenterer ikke i sig selv anonymitet eller lovlig behandling. [16]

10. Konkrete anbefalinger, hvis lovforslaget videreføres

Hvis lovgiver viderefører forslaget trods de grundlæggende indsigelser, anbefaler jeg som minimum følgende ændringer. De skal beskytte borgerne i den ordning, lovgiver vælger; de er ikke en tilslutning fra min side.

A. Dokumentation som betingelse for § 3

§ 3 bør gøre en dokumenteret beslutning til betingelse for behandlingsstart. Den skal omfatte det konkrete formål, nødvendigheden, lovlig opbevaring, hele forløbet gennem systemer og leverandører samt placeringen af ansvaret. Påkrævede risikovurderinger og konsekvensanalyser skal være afsluttet, og de nødvendige beskyttelser skal være gennemført. Dokumentationen skal også vise, hvordan borgernes rettigheder håndteres, og ajourføres ved væsentlige ændringer.

Bemærkningerne bør fastslå, at kravet omfatter udvikling og test, og at en generel analyse kan genbruges, når dens faktiske forudsætninger dokumenteret dækker den konkrete behandling. Dokumentationens omfang skal afpasses efter behandling og risiko.

B. Garantier før behandling efter § 3, stk. 2

De yderligere retlige garantier, som databeskyttelsesreglerne kræver, skal være fastsat og gælde, før behandlingen begynder. Myndigheden skal dokumentere, hvilke garantier der gælder, og hvordan de er gennemført. Interne politikker bør ikke stå alene, hvor beskyttelsen skal sikres ved lovgivning.

Hertil bør føjes bindende minimumskrav for andre indgribende anvendelser som beskrevet i afsnit 5, også når oplysningerne ikke er omfattet af artikel 9 og 10.

C. Afgrænsning af § 4

§ 4 bør kræve en konkret begrundelse for enhver rettighedsbegrænsning og en dokumenteret undersøgelse af mindre indgribende muligheder. Reglerne skal angive, hvilke rettigheder, behandlinger og personer de omfatter, hvor længe begrænsningen gælder, og hvordan den bliver efterprøvet. Systemets indretning, præcision eller omkostningerne ved at opfylde rettighederne må ikke alene begrunde begrænsningen.

Kravene skal gælde tilsvarende for regler udstedt af Domstolsstyrelsen, under respekt for domstolenes uafhængighed og de gældende kompetenceforhold.

D. § 5 og opfølgning

Lovforslaget foreslår ikrafttræden dagen efter bekendtgørelsen i Lovtidende. Det ophæver ikke GDPR's krav om, at behandlingen skal være lovlig fra start, men efterlader meget lidt tid til at omsætte nye bindende rammer til praksis. [1, § 5]

Jeg anbefaler en fastsat senere ikrafttrædelsesdato og om nødvendigt en trinvis ordning. Behandlinger, som kræver yderligere retlige garantier, bør først kunne støttes på loven, når garantierne er trådt i kraft. Vejledning, nødvendige bekendtgørelser og praktiske dokumentationskrav bør være tilgængelige inden da. En overgangsordning må ikke udskyde forpligtelser, der allerede følger af GDPR.

Jeg foreslår en offentlig evaluering senest to år efter ikrafttrædelsen med oplysninger om anvendelser, rettighedsbegrænsninger, klager, væsentlige hændelser og erfaringer med menneskelig kontrol.

11. Samlet anbefaling og anmodning til ministeriet

Jeg henstiller, at lovforslaget ikke vedtages i sin foreliggende form. Jeg er imod den brede adgang til AI-behandling af borgernes personoplysninger. Fuld anonymitet er for mig en forudsætning, og mine konkrete forslag til beskyttelse ændrer ikke dette standpunkt.

Jeg beder ministeriet forholde sig særskilt til anonymitet og genidentifikation, brugen af historiske data til nye formål, beskyttelsen af borgernes rettigheder og den reelle menneskelige kontrol. De beskrevne myndighedseksempler viser, hvorfor generelle henvisninger til eksisterende regler ikke er et tilstrækkeligt svar. De relevante oplysninger er gengivet i teksten med dato og kilde, så indsigelserne kan forstås uden kendskab til de underliggende aktindsigtssager.

Med venlig hilsen
Morten Larsen

Kilder og dokumentation

Vurderinger og anbefalinger er mine egne. Sidehenvisninger følger kildens egen sidenummerering, medmindre andet er angivet. Offentlige netkilder er linket. Dokumenter modtaget ved aktindsigt er identificeret med myndighed, dato og journalnummer; de relevante oplysninger er beskrevet i høringssvaret.

[1] Høringsgrundlag. Forsknings-, Uddannelses- og Digitaliseringsministeriet, *Forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)*, revideret høringsudkast, offentliggjort 14. september 2026, 81 sider. Digitaliseringsstyrelsens høringsbrev af samme dato, 3 sider. Høringsportalen, høring 71477.

[2] GDPR. Europa-Parlamentets og Rådets forordning (EU) 2016/679, navnlig betragtning 26 og 71 samt artikel 4, 5, 6, 9, 10, 12-23, 24-26, 28, 32, 35-36 og 44-49. Officiel tekst på EUR-Lex.

[3] Datatilsynets tidligere høringssvar. *Høring over udkast til forslag til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning*, 3. marts 2026, j.nr. 2026-11-0479, dok.nr. 840361, 15 sider, især s. 1-3 og 8-15.

[4] Databeskyttelse gennem design. EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, version 2.0, vedtaget 20. oktober 2020, navnlig pkt. 1-2, 13-16 og 35-38. Offentliggørelse og dokument.

[5] Begrænsninger af rettigheder. EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, vedtaget 13. oktober 2021, version 2.1 med formateringsændring 15. marts 2022, navnlig afsnit 3.2, 3.3.3, 3.5 og 4. Offentliggørelse og dokument.

[6] AI-modellers anonymitet. EDPB, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, vedtaget 17. december 2024, navnlig afsnit 3.2. Offentliggørelse og dokument.

[7] STARs afgørelse. Styrelsen for Arbejdsmarked og Rekruttering, *Afgørelse om aktindsigt i underbilag til konsekvensanalyserne for DFDG og DSDW samt anmodning om aktindsigt i øvrige dokumenter vedr. DFDG og DSDW*, 4. september 2026, j.nr. 2026-10734, s. 8-9. Aktindsigtsdokument.

[8] STARs slettepolitik. STAR, akt 12, *DOA-1A - Indsamler personoplysninger (opbevaring og strukturering) til DSDW*, sagsnr. 2025-12500, oprettet 9. december 2024, ajourført 1. oktober 2025, godkendt 12. januar 2026, s. 3-5, navnlig pkt. 10 og 13. Udleveret i aktindsigt i sag 2026-10734.

[9] Copilot. Økonomistyrelsen og Statens IT, *Konsekvensanalyse af Microsoft Copilot for Microsoft 365*, version 2.0, 23. februar 2026, 245 sider, her anvendt s. 225-229 om gennemførelse af foranstaltninger og DPO'ens bemærkninger. Aktindsigtsdokument.

[10] SSI. Statens Serum Institut, *Fuld imødekommelse af anmodning om aktindsigt*, 24. september 2026, j.nr. 26/02556, 7 sider, her navnlig de fysiske s. 6-7 om status for BSIG-notat og særskilt konsekvensanalyse. Afgørelsen beskriver notatet og konsekvensanalysen som foreløbige og ikke endeligt kvalitetssikrede.

[11] Irsk tilsynserfaring. Data Protection Commission, *Responsible Artificial Intelligence Innovation - Insights from the Data Protection Commission's Supervision of AI (2021-2025)*, september 2026, offentliggjort 24. september 2026. Her anvendt rapportens trykte s. 37-40, 49-50 og 59. Officiel offentliggørelse og rapport.

[12] STARs opdatering. Styrelsen for Arbejdsmarked og Rekruttering, Ny afgørelse af 30. september 2026, j.nr. 2026-3345, 12 sider, navnlig s. 6 om implementeret automatisk sletning i DFDG. Aktindsigtsdokument.

[13] Udledning af personlige egenskaber. Robin Staab, Mark Vero, Mislav Balunović og Martin Vechev, Beyond Memorization: Violating Privacy via Inference with Large Language Models, ICLR 2024. Officiel publikation.

[14] Genidentifikation med websøgning. Jianing Wen og Tianshi Li, AgentDoxx: Agentic Re-identification of Anonymized Text with Web Search, arXiv:2610.05586, version 1, 4. oktober 2026. Preprint. Publikation på arXiv.

[15] Datatilsynets aktuelle udmelding. Datatilsynet afgiver høringssvar til nyt udkast om AI-hjemmelslov, nyhed, 12. oktober 2026. Officiel nyhed.

[16] Offentlig registrering af AI-systemer. Forordning (EU) 2024/1689 med ændringer, artikel 49 og 71. Europa-Kommissionens opdaterede artikeltekster, kontrolleret 12. oktober 2026. Artikel 49. Artikel 71.

Til: Digitaliseringsstyrelsen (jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk, kahevi@digst.dk)
Fra: Nikolaj Deutch, cand.scient.pol. (privatperson), deutchnikolaj@gmail.com
Dato: 12. oktober 2026

Høringssvar: Udkast til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Jeg støtter, at der skabes et klart retsgrundlag for offentlige myndigheders brug af AI. Mine tre forslag skal gøre det muligt at efterprøve, at intentionerne i lovforslagets egne bemærkninger faktisk overholdes. Til hvert forslag har jeg vedlagt et forslag til formulering.

1. Logning, så den menneskelige vurdering kan rekonstrueres

Bemærkningerne (s. 19) anfører, at kravet til menneskelig involvering kan understøttes ved at "sikre relevant logning af anvendelsen af AI-systemet", men tilføjer: "Det bemærkes dog, at sådanne understøttende procedurer ikke i sig selv er et krav efter denne lovgivning." Jeg foreslår, at logning gøres til et krav, så det i den enkelte sag kan rekonstrueres, hvilket output AI-systemet leverede, og hvordan sagsbehandleren forholdt sig til det.

Kravet er ikke en ny type byrde. Det er en naturlig forlængelse af notatpligten i offentlighedslovens § 13 og svarer til de logkrav, AI-forordningen allerede stiller til højrisikosystemer (artikel 12 og artikel 26, stk. 6). Forslaget udstrækker blot princippet til de AI-systemer, som denne lov giver hjemmel til, uanset om de er højrisikosystemer.

Kravet er særlig vigtigt, fordi borgerens rettigheder efter databeskyttelsesforordningens artikel 12 og 15-21 kan begrænses efter lovudkastets § 4. Når borgerens egen indsigt begrænses, er klageinstanser, Folketingets Ombudsmand, domstolene og Datatilsynet den vigtigste kontrol, og de kan kun efterprøve det, der kan rekonstrueres.

> **Forslag til formulering:**
> *Myndigheden skal sikre logning af anvendelsen af AI-systemet, så det i den enkelte sag kan rekonstrueres, hvilken modelversion, hvilke inddata og hvilket output der indgik i sagen, hvornår det skete, og hvordan sagsbehandleren forholdt sig til outputtet. Logoplysningerne skal opbevares, så længe afgørelsen kan påklages eller indbringes for domstolene, og skal på anmodning stilles til rådighed for klageinstanser, Folketingets Ombudsmand, domstolene og tilsynsmyndigheden.*

2. Dokumenteret, uafhængig test før ibrugtagning og ved væsentlige ændringer

Myndigheden bør dokumentere, at AI-systemets output understøtter overholdelsen af forvaltningsrettens grundkrav, før systemet tages i brug, og når den underliggende model skiftes eller ændres væsentligt. Eksempler er begrundelse (forvaltningslovens §§ 22-24), klagevejledning (§ 25), partshøring (§ 19) og lighed, dvs. at ens sager behandles ens.

Testen bør udføres uafhængigt af både leverandøren og den enhed, der har udviklet eller anskaffet systemet, og testmetoden bør være offentlig. Ved at knytte kravet til væsentlige ændringer frem for enhver opdatering holdes byrden proportional.

Behovet følger af, hvordan AI-systemer fejler. En sagsbehandlers fejl rammer typisk én sag, mens en fejl i et AI-system rammer alle sager, der behandles på samme måde, og den kan være usynlig for den enkelte sagsbehandler. Når den underliggende model opdateres, ofte af leverandøren og uden for

myndighedens kontrol, kan systemets adfærd ændre sig, selv om myndighedens egen opsætning er uændret. Kun systematisk test kan afsløre den slags fejl, før de når borgerne.

> **Forslag til formulering:**
> *Før et AI-system tages i brug, og når den underliggende model skiftes eller ændres væsentligt, skal myndigheden dokumentere, at systemets output er testet for overensstemmelse med forvaltningsrettens krav, herunder krav om begrundelse, klagevejledning, partshøring og ligebehandling. Testen udføres uafhængigt af leverandøren og af den enhed, der har udviklet eller anskaffet systemet, efter en offentligt tilgængelig metode. Dokumentationen skal kunne forelægges tilsynsmyndigheden.*

3. Ét samlet tilsyn med ressourcer og en central testmetode

Loven bør udpege én navngiven myndighed, der fører tilsyn med, at kravene ovenfor overholdes, f.eks. Datatilsynet, som i forvejen fører tilsyn med offentlige myndigheders behandling af personoplysninger. Myndigheden bør tilføres de nødvendige ressourcer.

Tilsynet bør så vidt muligt samles med tilsynet efter lovforslag L 3 (2026-27) om supplerende bestemmelser til AI-forordningen. AI-forordningen regulerer systemerne som produkter, mens denne lov regulerer deres anvendelse i forvaltningen. Det er de samme systemer, og et samlet eller som minimum tæt koordineret tilsyn sikrer, at de ikke vurderes efter forskellige standarder.

Testmetoden bør fastsættes centralt, f.eks. af Digitaliseringsstyrelsen, som efter L 3 § 3 er centralt kontaktpunkt og koordinerer markedsovervågningsmyndighedernes samarbejde. L 3 § 9, stk. 3, fastsætter allerede, at markedsovervågningsmyndighederne "kan bistås af uafhængige sagkyndige" i forbindelse med tekniske undersøgelser. Samme model kan bruges til de uafhængige test.

> **Forslag til formulering:**
> *Datatilsynet fører tilsyn med, at kravene om logning og test i denne lov overholdes, og koordinerer tilsynet med de myndigheder, der fører tilsyn efter lov om supplerende bestemmelser til AI-forordningen. Digitaliseringsstyrelsen fastsætter efter forhandling med Datatilsynet en fælles metode for de uafhængige test.*

Jeg uddyber gerne forslagene.

Med venlig hilsen
Nikolaj Deutch

Til Digitaliseringsstyrelsen

Sendt pr. e-mail til jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk og kahevi@digst.dk

Aarhus, 11. oktober 2026

Høringssvar til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Vedr. Digitaliseringsstyrelsens høringsbrev af 14. september 2026.

Vi afgiver dette høringssvar på egne vegne. Vi er henholdsvis juridisk konsulent og AI-konsulent og arbejder til daglig med anvendelse af AI i kommunal opgavevaretagelse, fra den konkrete sagsbehandling til det politiske niveau.

Høringssvaret udtrykker vores egne faglige vurderinger. Vi er ikke opført på høringslisten og indsender svaret på eget initiativ.

Sammenfatning

Vi finder det positivt, at lovforslaget tilvejebringer en generel hjemmel til offentlige myndigheders anvendelse af AI-systemer. Vores bemærkninger kan sammenfattes i fire forslag:

1. § 3, stk. 1, eller bemærkningerne hertil præciseres, så det utvetydigt fremgår, at hjemlen også omfatter oplysninger omfattet af databeskyttelsesforordningens artikel 9 og 10 (afsnit 1).
2. § 3, stk. 2, ændres, så ressortministrene som udgangspunkt **skal** – og ikke blot **kan** – fastsætte passende og specifikke foranstaltninger ved behandling af disse oplysninger (afsnit 2).
3. Der stilles krav om løbende og systematisk evaluering af AI-systemers faktiske betydning for sagsbehandlingen og afgørelseskvaliteten, også for systemer, der ikke er højrisiko-AI-systemer efter AI-forordningen (afsnit 3).
4. Det overvejes at indføre en nærmere afgrænset hjemmel til automatiserede afgørelser, hvor borgeren gives fuldt medhold, med passende retssikkerhedsgarantier (afsnit 4).

1. Lovforslagets § 3, stk. 1 – hjemmel til behandling af artikel 9- og 10-oplysninger

Det fremgår af lovforslagets § 3, stk. 1, at offentlige myndigheder og organer kan udvikle og anvende AI-systemer på baggrund af personoplysninger, som myndigheden eller organet behandler, med henblik på at understøtte opgavevaretagelsen efter anden lovgivning.

Det bør efter vores opfattelse fremgå tydeligere af selve bestemmelsen, at hjemlen også omfatter behandling ved hjælp af AI-systemer af særlige kategorier af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, samt oplysninger om straffedomme og lovovertrædelser omfattet af artikel 10.

Det kan ganske vist udledes af § 3, stk. 2 og lovforslagets bemærkninger, at sådanne oplysninger forudsættes at kunne omfattes af loven. Det vil imidlertid styrke retssikkerheden og skabe større klarhed for de myndigheder og organer, der skal anvende bestemmelsen i praksis, hvis dette fremgår udtrykkeligt af hjemmelsbestemmelsen i § 3, stk. 1.

Det foreslås derfor, at § 3, stk. 1, eller bemærkningerne hertil præciseres, således at det utvetydigt fremgår, at bestemmelsen, under iagttagelse af databeskyttelsesforordningens øvrige betingelser, også kan danne grundlag for anvendelse af AI-systemer ved behandling af oplysninger omfattet af artikel 9 og 10.

2. Lovforslagets § 3, stk. 2 – krav om passende og specifikke foranstaltninger

Efter lovforslagets § 3, stk. 2, **kan** vedkommende minister på eget ressort fastsætte passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser, når behandlingen omfatter oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10.

Det bør overvejes, om bestemmelsen i stedet bør fastsætte, at vedkommende minister **skal** fastsætte sådanne passende og specifikke foranstaltninger.

Oplysninger omfattet af artikel 9 og 10 er efter deres karakter særligt beskyttelsesværdige, og anvendelsen af disse oplysninger i AI-systemer kan indebære særlige risici for de registreredes rettigheder og interesser. Når der med lovforslaget

etableres en generel hjemmel, som kan anvendes på tværs af den offentlige sektor, bør der derfor samtidig være sikkerhed for, at der på de enkelte ressortområder tages konkret stilling til, hvilke supplerende beskyttelsesforanstaltninger der er nødvendige.

Anvendelsen af ordet **"kan"** indebærer en risiko for, at der på enkelte ressortområder ikke fastsættes yderligere foranstaltninger, selv om AI-systemer anvendes til behandling af meget beskyttelsesværdige oplysninger. Dette kan føre til forskelle i beskyttelsesniveauet på tværs af den offentlige sektor og skabe usikkerhed om, hvilke sikkerheds- og retssikkerhedsmæssige krav der gælder.

Det bemærkes i den forbindelse, at lovbemærkningerne allerede anfører, at der vil være en forpligtelse til at fastsætte specifikke foranstaltninger i de tilfælde, hvor dette er påkrævet efter databeskyttelsesreglerne. Det vil efter vores opfattelse være mere hensigtsmæssigt, at denne forpligtelse afspejles tydeligt i selve lovteksten.

Det foreslås derfor, at § 3, stk. 2 ændres, således at ressortministerierne som udgangspunkt skal fastsætte passende og specifikke foranstaltninger ved behandling af oplysninger omfattet af artikel 9 og 10. Hvis der allerede følger tilstrækkelige og passende foranstaltninger af den relevante sektorlovgivning, vil bestemmelsen eventuelt kunne udformes således, at der ikke skal fastsættes yderligere foranstaltninger, når det konkret kan konstateres, at det nødvendige beskyttelsesniveau allerede er sikret.

En sådan løsning vil efter vores opfattelse skabe en bedre balance mellem lovforslagets formål om at etablere en bred og anvendelig hjemmel til brug af AI i den offentlige sektor og hensynet til den særlige beskyttelse, som behandling af oplysninger omfattet af artikel 9 og 10 nødvendiggør.

3. Evaluering og kvalitetssikring af AI-systemer

Lovforslaget fremhæver bl.a. referatskrivning, journalisering, tale-til-tekst-løsninger og chatbots som eksempler på anvendelser, hvor AI kan bidrage til en mere effektiv offentlig opgavevaretagelse. Det er positivt, at der med lovforslaget tilvejebringes en generel hjemmel til sådanne anvendelser.

Det bør imidlertid overvejes, om lovforslaget i tilstrækkelig grad adresserer de retssikkerheds- og kvalitetsmæssige risici, der kan opstå ved anvendelsen af AI-systemer, som ikke nødvendigvis er klassificeret som højrisiko-AI-systemer efter AI-forordningen.

Et AI-system kan eksempelvis have en høj teknisk nøjagtighed ved transskribering uden nødvendigvis at sikre et retvisende grundlag for den efterfølgende myndighedsudøvelse. Et tale-til-tekst-system kan således systematisk gengive bestemte oplysninger, nuancer

eller udsagn på en måde, som påvirker sagsoplysningen og i sidste ende myndighedens afgørelser. En isoleret måling af systemets tekniske præcision er derfor ikke nødvendigvis tilstrækkelig til at vurdere systemets faktiske betydning for kvaliteten af myndighedens opgavevaretagelse.

Lovforslaget fremhæver bl.a. kortere sagsbehandlingstid, øget ensartethed og højere kvalitet som mulige gevinster ved anvendelsen af AI. Det bør på den baggrund overvejes at stille krav om, at sådanne effekter løbende og systematisk evalueres, navnlig hvor AI-systemets output indgår i grundlaget for myndighedens afgørelser eller øvrige myndighedsudøvelse.

En sådan evaluering bør ikke alene rette sig mod AI-systemets tekniske performance, men også mod konsekvenserne for den efterfølgende sagsbehandling og afgørelseskvalitet. For et referat- eller transskriptionsværktøj vil det eksempelvis kunne indebære stikprøvekontrol, sammenligning af sager behandlet med og uden anvendelse af AI samt kontrol med, om anvendelsen medfører systematiske afvigelser eller nye fejltyper.

Dette vil kunne supplere de krav, der allerede følger af bl.a. databeskyttelsesreglerne, almindelige forvaltningsretlige principper og, hvor systemet er omfattet heraf, AI-forordningens krav. Det er særligt relevant for AI-systemer, som kan have væsentlig faktisk betydning for myndighedens sagsbehandling, men som ikke omfattes af AI-forordningens særlige krav til højrisiko-AI-systemer.

4. Automatiserede medholdsafgørelser

Det bør samtidig overvejes, om lovforslaget i videre omfang kan skabe hjemmel til automatiseret afgørelsesvirksomhed i nærmere afgrænsede situationer.

En mulighed kunne være afgørelser, hvor borgeren gives fuldt medhold, og hvor sagen i øvrigt er egnet til automatiseret behandling. Forvaltningslovens begrundelseskrav gælder som udgangspunkt ikke, når afgørelsen fuldt ud giver den pågældende part medhold, jf. forvaltningslovens § 22. Databeskyttelsesforordningens artikel 22 udelukker heller ikke i alle tilfælde automatiske individuelle afgørelser, idet sådanne afgørelser bl.a. kan tillades ved EU-ret eller national ret, når der samtidig fastsættes passende foranstaltninger til beskyttelse af den registreredes rettigheder, frihedsrettigheder og legitime interesser.

Hvis lovgiver ønsker at åbne mulighed for sådanne automatiserede afgørelser, bør det derfor ske inden for klart definerede rammer og med relevante retssikkerhedsgarantier.

En central garanti vil i den forbindelse kunne være krav om dokumenteret og systematisk evaluering af systemets præcision og fejlrate inden ibrugtagning og løbende under anvendelsen. Testgrundlaget bør være tilstrækkeligt omfattende og repræsentativt til, at myndigheden med den fornødne sikkerhed kan vurdere risikoen for fejlagtige afgørelser. Det vil således ikke nødvendigvis være tilstrækkeligt, at der ikke konstateres fejl i en begrænset stikprøve.

Automatisering vil navnlig kunne være relevant i klare og ensartede sagstyper, hvor systemet alene kan træffe en automatisk afgørelse, hvis betingelserne for fuldt medhold med tilstrækkelig sikkerhed er opfyldt. Sager, hvor betingelserne ikke entydigt er opfyldt, bør i stedet overgå til almindelig manuel sagsbehandling. Det samme gælder sagstyper, hvor der eksempelvis indgår modstående partsinteresser, skønsmæssige vurderinger eller fordeling af begrænsede ressourcer.

En sådan model vil kunne indebære en anden effektiviseringsgevinst end traditionel beslutningsstøtte. Ved beslutningsstøtte skal den ansvarlige medarbejder fortsat foretage en reel og selvstændig vurdering af den enkelte sag. Ved en forsvarligt afgrænset automatisering af klare medholdssager vil den manuelle sagsbehandling derimod kunne koncentreres om de sager, hvor der faktisk er behov for en konkret faglig eller juridisk vurdering.

Det foreslås derfor, at lovforslaget både indeholder krav om systematisk evaluering af AI-systemers faktiske betydning for afgørelseskvaliteten og overvejer en nærmere afgrænset hjemmel til automatiserede medholdsafgørelser med passende retssikkerhedsgarantier.

Vi står gerne til rådighed for at uddybe vores bemærkninger.

Med venlig hilsen

Sarah Kaagaard Dahl, cand.jur.
Juridisk konsulent
sarahkadahl@gmail.com · 60384525

Jakob Mørup Wang, cand.scient.
AI-konsulent
jakobmwang@gmail.com · 61656964

Til: jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk, kahevi@digst.dk
Fra: Tony Bidstrup (tonybidstrup@gmail.com)
Titel: Bemærkninger til udkastet til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning
Sendt: 05-10-2026 21:41

[EKSTERN E-MAIL] Denne e-mail er sendt fra en ekstern afsender.
Vær opmærksom på, at den kan indeholde links og vedhæftede filer, som ikke er sikre.

Kære Digitaliseringsstyrelsen,

Dato: 5/10 -2026

Jeg fremsender hermed mine bemærkninger til udkastet til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning.

Min væsentligste bekymring vedrører grænsen mellem beslutningsstøtte og automatiske afgørelser. Hertil kommer forslagets brede adgang til videreanvendelse af personoplysninger og muligheden for at begrænse borgernes databeskyttelsesrettigheder.

1. Beslutningsstøtte og risikoen for rent formel menneskelig godkendelse

Efter § 2, nr. 4, omfatter beslutningsstøtte forslag eller anbefalinger til afgørelser eller tiltag, som en fysisk person inddrager i den samlede faglige vurdering, uden at AI-systemet selv træffer afgørelsen eller iværksætter tiltaget.

Denne definition efterlader efter min opfattelse et væsentligt spørgsmål: Hvad forhindrer i praksis en sagsbehandler i blot at godkende AI-systemets anbefaling, uden at foretage en reel og selvstændig vurdering?

At et menneske formelt godkender resultatet, dokumenterer ikke i sig selv, at afgørelsen er truffet på grundlag af en selvstændig menneskelig vurdering. Under tidspres eller ved stor tillid til systemet kan godkendelsen blive en rutinemæssig handling.

Grænsen kan heller ikke fastlægges ud fra, om sagsbehandleren ændrer et ord eller en sætning. Sproglige ændringer kan foretages uden nogen efterprøvelse af konklusionen. Omvendt kan en grundig, selvstændig vurdering føre til samme resultat som AI-systemets anbefaling.

Artikel 29-gruppens vejledning om automatiske individuelle afgørelser og profilering, WP251rev.01, revideret den 6. februar 2018, side 21, understreger, at menneskelig involvering ikke må konstrueres for at undgå GDPR artikel 22. Kontrollen skal være reel og foretages af en person med kompetence og beføjelse til at ændre resultatet.

Jeg anmoder derfor om, at loven udtrykkeligt stiller krav om reel, selvstændig og dokumenteret menneskelig vurdering. Ren godkendelse og kosmetiske ændringer bør ikke være tilstrækkelige til at betegne processen som beslutningsstøtte.

Sagsbehandleren skal have den nødvendige tid, faglige kompetence og adgang til grundlaget for anbefalingen samt reel mulighed for at tilsidesætte den. Vurderingen skal omfatte sagens relevante faktiske oplysninger, borgerens indsigelser og det retlige grundlag.

2. Dokumentation og mulighed for at anfægte afgørelsen

Det er positivt, at bemærkningerne fastslår, at almindelige forvaltningsretlige regler og principper fortsat gælder. Det bør imidlertid konkretiseres, hvordan disse rettigheder sikres, når AI indgår i sagsbehandlingen.

Jeg foreslår et udtrykkeligt krav om, at det dokumenteres i sagen, ***når AI har haft betydning for en afgørelse eller et tiltag*.** Dokumentationen bør omfatte de anvendte oplysninger, systemets relevante output, systemets version og sagsbehandlerens efterprøvelse.

Borgeren bør oplyses om AI-systemets rolle og have adgang til en forståelig forklaring på de forhold, som har påvirket resultatet. En klageinstans eller domstol skal tilsvarende kunne efterprøve både anbefalingens grundlag og den menneskelige vurdering.

Borgeren bør ikke stilles i en situation, hvor vedkommende skal påvise manglende menneskelig vurdering, mens dokumentationen alene befinder sig hos myndigheden eller slet ikke er bevaret.

3. Videreanvendelse af personoplysninger til AI-udvikling

Det fremgår af bemærkningerne til § 3, side 57, at oplysninger indsamlet til eksempelvis konkret sagsbehandling vil kunne anvendes til udvikling af AI-systemer, uden at myndigheden skal foretage en nærmere vurdering af, om formålene er forenelige.

Dette er en vid adgang, som bør afgrænses tydeligere. Oplysninger, som borgeren har afgivet for at få behandlet en konkret sag, kan være både følsomme og tæt knyttet til borgerens private forhold.

Jeg anmoder om klare krav til udviklingsformål, nødvendighed, dataminimering, opbevaring og beskyttelse af oplysningerne. Det bør desuden dokumenteres, hvorfor udviklingen ikke kan gennemføres med anonyme eller mindre omfattende data.

4. Begrænsninger af borgernes rettigheder

Efter § 4 kan vedkommende minister fastsætte undtagelser fra GDPR artikel 12 og 15–21. Bemærkningerne åbner desuden for begrænsninger på hele sektorområder.

Jeg finder det betænkeligt, at så væsentlige spørgsmål om blandt andet indsigt, berigtigelse og sletning i dette omfang overlades til efterfølgende ministerielle regler.

GDPR artikel 23 kræver, at begrænsninger er nødvendige og proportionale og respekterer rettighedernes væsentligste indhold. Jeg anmoder om, ***at loven selv fastlægger tydeligere grænser for bemyndigelsen og krav om offentlig begrundelse, afgrænset varighed og regelmæssig revurdering.***

AI-systemers tekniske opbygning bør ikke i sig selv begrunde en begrænsning af borgernes rettigheder. Før en begrænsning indføres, bør det dokumenteres, at mindre indgribende tekniske og organisatoriske løsninger er undersøgt. Systemerne bør fra begyndelsen indrettes, så rettighederne kan efterleves.

5. Fejl og forskelsbehandling

Bemærkningerne på side 37–38 erkender risikoen for, at ***AI-systemer kan videreføre eller forstærke forskelsbehandling.***

Jeg anmoder om, at det præciseres, hvordan risikoen skal undersøges før ibrugtagning og overvåges under anvendelsen, samt hvilke supplerende garantier der er nødvendige ud over de eksisterende regler.

Der bør være klare procedurer for at standse eller begrænse anvendelsen ved systematiske fejl, rette berørte afgørelser og identificere borgere, som kan være blevet ramt. Ansvaret for at reagere skal være tydeligt placeret hos myndigheden.

6. Afslutning.

Jeg støtter anvendelsen af kunstig intelligens som redskab til at styrke den juridiske kvalitet i myndighedernes sagsbehandling. AI kan eksempelvis anvendes til at gennemgå udkast til afgørelser og gøre opmærksom på mulige retlige fejl, mangelfulde begrundelser, oversete oplysninger eller relevant lovgivning og praksis. En sådan anvendelse kan bidrage til at styrke borgernes retssikkerhed, forudsat at systemets resultater efterprøves fagligt.

Jeg vil derimod fraråde, at AI-systemer udvikles eller anvendes til at anbefale udfaldet af konkrete borgeres sager, fordi anbefalingen risikerer at blive styrende for sagsbehandlerens vurdering.

Når myndighedernes adgang til at anvende AI udvides, skal borgernes mulighed for indsigt, kontrol og retlig prøvelse sikres tilsvarende.

Hvis adgangen til at anvende AI til sådanne anbefalinger fastholdes, anmoder jeg navnlig om, at § 2, nr. 4, præciseres, så en formel menneskelig godkendelse ikke kan træde i stedet for en reel og selvstændig vurdering. ***Det skal kunne dokumenteres og efterprøves, at sagsbehandleren selvstændigt har vurderet sagens faktiske og retlige grundlag*** og ikke blot har godkendt AI-systemets anbefaling.

Jeg anmoder om, at ovenstående bemærkninger indgår i den videre behandling af lovforslaget og besvares i høringsnotatet.

Med venlig hilsen,
Tony Bidstrup
Rødager Alle 58 st.tv
2610 Rødovre

- HØRINGSSVAR

Dansk Erhverv

Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Dansk Erhverv takker for muligheden for at afgive høringssvar til udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven).

Sammenfatning

Dansk Erhverv støtter lovforslaget, som er et vigtigt skridt mod klarere rammer for brugen af AI i den offentlige sektor. Vores tre vigtigste pointer er:

- **Fravær af bekendtgørelse må ikke blokere for brugen af loven.** Det bør tydeliggøres, hvordan behovet for beskyttelsesforanstaltninger efter § 3, stk. 2, vurderes, når en behandling ikke kan henføres til ét ressortområde. Det bør også fremgå klart, at § 3 kan anvendes uden en bekendtgørelse, når behandlingen i øvrigt har det nødvendige retsgrundlag og tilstrækkelige beskyttelsesforanstaltninger.
- **Teknologineutral regulering.** Kravet til retsgrundlaget bør afhænge af, hvor indgribende behandlingen er, og ikke af om løsningen er et AI-system.
- **Vejledningen skal foreligge før ikrafttrædelsen.** Loven træder i kraft dagen efter bekendtgørelsen. Der bør derfor være klarhed om anvendelsen fra første dag..

Generelle bemærkninger

Lovforslaget er et vigtigt skridt i den rigtige retning. I lang tid har både myndigheder og leverandører holdt igen med AI, fordi det har været uklart, hvad der reelt var lovligt. Det skyldes ikke mindst Datatilsynets praksis, hvor indgribende brug af AI i visse tilfælde kræver et klarere retsgrundlag end anden teknologi. Hjemlerne er derfor blevet skabt én lov ad gangen. Resultatet er et uensartet retsgrundlag og løsninger, der er blevet forsinket eller aldrig er kommet i drift.

Det er en udfordring, fordi den offentlige sektor skal blive langt bedre til at bruge digitale værktøjer, hvis der skal frigøres tid til kernevelfærd og samtidig løftes kvalitet i sagsbehandling og service. Her kan AI give bedre overblik, hurtigere sagsoplysning og mere ensartede vurderinger, men kun hvis juraen ikke står i vejen.

Lovforslaget giver de klare rammer, der skal til. Myndighederne får et fælles udgangspunkt, og virksomhederne bag løsningerne får mere forudsigelighed.

Samspillet mellem § 3, stk. 1, og § 3, stk. 2

Efter § 3, stk. 2, kan vedkommende minister fastsætte passende og specifikke foranstaltninger, når behandlingen omfatter oplysninger omfattet af databeskyttelsesforordningens artikel 9 eller 10. Det fremgår af bemærkningerne, at sådanne foranstaltninger i visse tilfælde skal være fastsat, før behandlingen kan ske lovligt.

Ordningen forudsætter, at behandlingen kan henføres til et bestemt ressortområde og en bestemt sektorlov. Det er ikke altid tilfældet. I kommunal praksis kan forebyggende indsatser og den tilhørende behandling af personoplysninger hvile på flere bestemmelser på én gang, herunder de almindelige forvaltningsretlige forpligtelser om sagsoplysning og vejledning. Her kan det være vanskeligt at placere behandlingen under én ministers ressort eller én specifik lov, som en bekendtgørelse normalt vil skulle henvise til.
Bemærkningerne peger på, at flere ministre kan udstede en fælles bekendtgørelse, når en opgave ikke entydigt kan henføres til ét ressortområde. Det forudsætter dog, at de relevante ressorter kan identificeres, og en fælles bekendtgørelse kræver koordinering mellem

flere ministerier. Det kan tage tid, og i mellemtiden står kommunerne uden afklaring af, om de kan anvende loven.

Dansk Erhverv foreslår derfor:

- at lovbemærkningerne eller en vejledning til loven beskriver, hvordan behovet for beskyttelsesforanstaltninger skal vurderes i tværgående tilfælde, og hvem der har ansvaret for vurderingen
- at det fremgår klart, at fraværet af en bekendtgørelse ikke i sig selv hindrer anvendelse af § 3, hvis behandlingen i øvrigt har det nødvendige retsgrundlag, og der er etableret tilstrækkelige beskyttelsesforanstaltninger.

Uden en sådan afklaring kan der fortsat opstå usikkerhed om den praktiske anvendelse af loven, selv om det generelle retsgrundlag er på plads.

Teknologineutralitet

Dansk Erhverv anbefaler, at reguleringen udformes mere teknologineutralt.
Databeskyttelsesreglerne er teknologineutrale, og det afgørende bør være, hvor indgribende en behandling er for borgeren – ikke hvilken teknologi der anvendes. Det anerkendes også i lovforslagets bemærkninger. Alligevel knytter lovforslaget hjemlen til AI-forordningens definition af et AI-system.

Det kan skabe en ny grænsedragning, hvor myndighederne først skal afgøre, om en løsning er et AI-system eller f.eks. en regelbaseret algoritme eller anden avanceret dataanalyse, før de ved, om loven kan anvendes. Samtidig risikerer loven at skulle ændres, i takt med at teknologien udvikler sig.

Dansk Erhverv foreslår, at det overvejes at lade hjemlen omfatte digitale beslutningsstøtteværktøjer mere bredt. Som minimum bør det fremgå af bemærkningerne, at kravet til retsgrundlaget for andre digitale værktøjer fortsat vurderes ud fra behandlingens indgribende karakter og ikke ud fra den anvendte teknologi.

Klinisk AI i sundhedsvæsenet

AI i sundhedsvæsenet bør behandles som et selvstændigt område i loven. En stor del af den AI, der i dag anvendes i sundhedsvæsenet, er CE-mærket medicinsk udstyr. Efter MDR skal software, der er beregnet til at diagnosticere, forebygge, lindre eller behandle sygdom, handicap eller skade, CE-mærkes som medicinsk udstyr. Klinisk AI er dermed allerede underlagt en omfattende regulering, der håndterer risikoen ved anvendelsen. Det gælder også, når løsningen er autonom.

Autonom AI er CE-mærket medicinsk udstyr, der inden for sit godkendte formål udfører en afgrænset klinisk opgave, uden at en sundhedsperson vurderer hvert enkelt tilfælde. Typisk frasorterer systemet de normale fund, så speciallægerne kan bruge deres tid på de patienter, der har brug for dem. Flere autonome løsninger er allerede CE-mærket og i brug i andre europæiske lande, bl.a. inden for røntgen, dermatologisk billeddiagnostik og øjenundersøgelser. Antallet af undersøgelser stiger, og der mangler speciallæger. Autonom AI er derfor en af de få veje til mere kapacitet i sundhedsvæsenet uden lavere kvalitet.

I Danmark er autonom drift i dag reelt udelukket, og regionerne er henvist til beslutningsstøtte, hvor en læge ser hvert svar. Barrieren er manglende hjemmel. EU-Domstolen har i SCHUFA-dommen (C-634/21) fastslået, at databeskyttelsesforordningens artikel 22 indeholder et principielt forbud mod afgørelser, der alene er baseret på automatisk behandling. Forbuddet kan fraviges, hvis afgørelsen har hjemmel i national ret med passende garantier (artikel 22, stk. 2, litra b). For helbredsoplysninger kræves desuden hjemmel efter artikel 9, stk. 2, litra g. En sådan hjemmel findes ikke i dansk ret i dag. Dansk Erhverv mener, at den bør gives med dette lovforslag.

De passende garantier findes allerede

- **CE-mærkning.** Før markedsføring skal fabrikanten dokumentere klinisk evidens for netop det tiltænkte formål. For udstyr i klasse IIa og derover skal et bemyndiget organ godkende dokumentationen. Lægemiddelstyrelsen fører markedsovervågning, hændelser skal indberettes, og fabrikanter, importører og distributører skal registreres. En godkendt model er "låst". Den lærer ikke af den enkelte patient og giver samme svar på samme input. Ændringer i modellen kræver en ny overensstemmelseserklæring, og ved væsentlige ændringer skal løsningen igen forbi et bemyndiget organ.
- **AI-forordningen.** AI i medicinsk udstyr, der skal vurderes af et bemyndiget organ, er højrisiko efter AI-forordningen. Kommissionen har i sit forslag til revision af MDR lagt op til, at AI-forordningens krav integreres direkte i MDR. Det støtter Dansk Erhverv. Den politiske aftale udestår, men uanset udfaldet vil AI i medicinsk udstyr være underlagt de højeste sikkerhedskrav i EU.
- **Idriftsætterrollen.** AI-forordningen placerer en række forpligtelser hos idriftsætteren, f.eks. et hospital eller en region, frem for hos den enkelte læge. Det gælder bl.a. overvågning og logning. Ansvaret for en autonom løsning kan dermed placeres hos f.eks. den lægefaglige ledelse.
- **Delegering er kendt praksis**. Efter autorisationslovens § 17 kan læger allerede i dag delegere opgaver til andre faggrupper med en konkret instruks og under tilsyn, mens ansvaret forbliver hos lægen. Et autonomt AI-setup kan ses på samme måde. Den lægefaglige ledelse godkender opsætning, kvalitetssikring, tærskelværdier og henvisningskriterier.

Lovforslaget forholder sig i dag ikke til, at klinisk AI er underlagt en selvstændig regulering, der sikrer patientsikkerheden. Det bør det gøre. Det er i tråd med princippet om teknologineutralitet. Kravene til retsgrundlaget bør afspejle, hvor indgribende behandlingen er, og hvilke garantier der allerede gælder. For klinisk AI er disse garantier omfattende.

Dansk Erhverv anbefaler derfor:

- at loven skelner mellem CE-mærket klinisk AI og øvrig offentlig AI, og at det anerkendes, at MDR, IVDR og AI-forordningen udgør passende garantier efter databeskyttelsesforordningen
- at der indføres en bestemmelse, der tillader automatiske afgørelser ved brug af CE-mærket medicinsk udstyr inden for dets godkendte autonome formål, jf. artikel 22, stk. 2, litra b, og artikel 9, stk. 2, litra g
- at det med henvisning til idriftsætterrollen i AI-forordningen fastslås, at menneskelig involvering kan ske på systemniveau gennem et organisatorisk ansvar hos en navngiven person for idriftsættelse og tilsyn

Beslutningsstøtte og menneskelig involvering

Bemærkningerne overlader det til praksis at fastlægge grænsen mellem beslutningsstøtte og fuldautomatiske afgørelser. Det er forståeligt, men skaber usikkerhed i en overgangsperiode. Dansk Erhverv opfordrer til, at der udarbejdes en vejledning til loven, som giver konkrete eksempler på, hvad en reel menneskelig vurdering indebærer, og hvordan den kan dokumenteres, f.eks. gennem logning og registrering af afvigelser fra systemets forslag.

En reel menneskelig vurdering forudsætter samtidig, at medarbejderne har både kompetencer og ressourcer til selv at træffe den endelige beslutning. Det kræver opkvalificering og tid i sagsbehandlingen til at forholde sig til systemets forslag. Det bør indgå i vejledningen og i myndighedernes implementering.

Menneskelig involvering kan i visse tilfælde ske på systemniveau frem for i den enkelte sag. Det er relevant, hvor et AI-system allerede er underlagt høje krav til dokumentation, kontrol og tilsyn, som det er tilfældet for CE-mærket klinisk AI, jf. afsnittet herom.

Offentligt-privat samarbejde

Udbredelsen af AI i den offentlige sektor forudsætter et stærkt samarbejde mellem myndigheder og private leverandører. Mange af løsningerne udvikles af virksomheder, og kvaliteten afhænger ofte af, at de løbende kan forbedres.

Lovforslaget giver hjemmel til, at myndigheden selv kan udvikle eller få udviklet AI-systemer på egne data. Det er mindre klart, hvilke muligheder der er for, at leverandører kan bidrage til at forbedre løsningerne på baggrund af erfaringer fra brugen. Dansk Erhverv anerkender, at der ofte er tale om oplysninger om borgere i sårbare situationer, og at hensynet til databeskyttelse og borgernes tillid skal veje tungt.

Dansk Erhverv opfordrer derfor til, at vejledningen beskriver, hvordan myndigheder og leverandører kan samarbejde om at udvikle og forbedre løsninger inden for databeskyttelsesreglerne. Det kan f.eks. ske gennem anonymisering og andre beskyttende teknikker, og ved at myndighederne stiller klare krav til leverandørerne i udbud og databehandleraftaler. Det vil give både myndigheder og leverandører et fælles grundlag at arbejde ud fra.

Vejledning

Loven træder efter § 5 i kraft dagen efter bekendtgørelsen i Lovtidende, så myndighederne hurtigt kan komme i gang. Det forudsætter, at der er klarhed om anvendelsen fra første dag. Dansk Erhverv anbefaler derfor, at vejledningen udarbejdes i dialog med relevante aktører og offentliggøres forud for lovens ikrafttrædelse, så myndigheder og leverandører kan forberede sig.

Dansk Erhverv står gerne til rådighed for en uddybning af høringssvaret.

Dansk Industri

Høringssvar fra Dansk Industri (DI)
Vedr.: Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Dansk Industri (DI) takker for muligheden for at afgive høringssvar til lovforslaget.

DI deler ambitionen om, at den offentlige sektor i langt højere grad skal kunne anvende digitale løsninger – herunder AI – til at øge kvaliteten, effektiviteten og ensartetheden i sagsbehandling og opgaveløsning. Lovforslaget adresserer en velkendt og væsentlig barriere: den manglende afklaring af et tilstrækkeligt klart databeskyttelsesretligt retsgrundlag for myndigheders behandling af personoplysninger ved brug af AI-systemer, bl.a. til beslutningsstøtte.

DI ser derfor positivt på, at der etableres en generel databeskyttelsesretlig hjemmel, som kan gøre det muligt for myndigheder at udvikle og anvende AI-systemer i deres opgavevaretagelse, herunder med brug af historiske sager som træningsdata, når det sker inden for rammerne af den i forvejen afgrænsede myndighedsopgave. DI understreger dog nødvendigheden af, at myndighedsopgaven forstås bredt, så lovforslaget også omfatter muligheden for at den offentlige forvaltning kan benytte kendte effektiviseringsværktøjer som tale-til-tekst, mailsortering og forskning.

Samtidig vurderer DI, at lovforslaget – i sin nuværende form – rummer risici for, at den juridiske usikkerhed og den praktiske anvendelighed ikke løses tilstrækkeligt. Der er især behov for at sikre, at hjemlen bliver **teknologineutral og tilstrækkelig bred**, at den ikke skaber unødig **fragmentering på tværs af ressortområder**, samt at rammerne for gennemsigtighed, ansvar og samarbejde med leverandører er klare og skalerbare.

Sidst bør lovforslaget i højere grad understøtte samarbejdet med det private erhvervsliv og dermed de leverandører, der skal udvikle løsningerne.

DI's hovedanbefalinger (kort)

DI anbefaler særligt, at:

1. Hjemlen udformes mere **teknologineutralt** og fremtidssikret, så den ikke kun omfatter "AI-systemer", men også tilsvarende digitale beslutnings- og arbejdsgangsstøttesystemer.

2. Hjemlen bør helt entydigt omfatte en adgang til at udvikle og anvende AI med det formål at effektivisere opgaveløsningen, driften mv. i den offentlige sektor og ikke videreføre den GDPR-afledte hjemmelsmæssige udfordring ved at koble anvendelse af AI op på "opgave-varetagelse efter anden lovgivning"

3. Afgrænsningen mellem **beslutningsstøtte** og **automatiserede afgørelser** præciseres operationelt og reducerer usikkerhed i myndighedernes ibrugtagning. Ministeriet bør fremadrettet undersøge, hvor brug af AI, der vil udgøre en automatisk afgørelse, vil kunne anvendes i det offentlige til at give værdi samtidig med at retten til privatliv beskyttes. I forlængelse heraf anbefaler DI, at ministeriet ikke på forhånd afskriver automatiserede afgørelser fuldstændigt, men i stedet undersøger mulighederne for automatiserede afgørelser på afgrænsede områder, hvor risikoen er acceptabel.

4. Der etableres et **fælles national katalog for krav/foranstaltninger** på tværs af sektorer for så vidt muligt at sikre strømlinede passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser i forbindelse med behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10, hvor sådanne passende og specifikke foranstaltninger er påkrævet, jf. § 3, stk. 2, jf. databeskyttelsesforordningens artikel 9, stk. 2.

5. Arbejdet med at identificere sektorområder, hvor yderligere passende og specifikke foranstaltninger er påkrævet, og udarbejde nødvendige supplerende tiltag, skal koordineres i en nedsat arbejdsgruppe.

6. Der skabes større klarhed om, hvordan hjemlen understøtter **samarbejdsmodeller med private leverandører**.

Generelle bemærkninger

1. Positivt med en generel hjemmel – men væsentligt at den tager højde for væsentlige udfordringer, der kan opstå i praksis

DI anerkender, at lovforslaget ikke ændrer på eksisterende krav i anden lovgivning (fx forvaltningsretlige krav) og at øvrige krav i databeskyttelsesretten fortsat skal overholdes, herunder eksempelvis krav om konsekvensanalyse (DPIA).

Det er positivt, at lovforslaget samlet set sigter mod at gøre det muligt for myndigheder at anvende AI-systemer på samme måde, som myndigheder i dag anvender andre elektroniske hjælpemidler i sagsbehandlingen.

DI fremhæver dog, at hvis lovforslaget skal løfte sin primære mission – at fjerne hjemmelsusikkerhed og gøre ansvarlig ibrugtagning mulig – skal hjemlen udformes, så den:

- er **fremtidssikret** (teknologineutral),
- er **skalerbar** på tværs af myndigheder og sektorer (fælles baseline),

- alene forudsætter, at der anvendes oplysninger, som myndigheden mv. allerede lovligt behandler **uden at det forudsættes**, at opgavevaretagelse (formålet) følger af anden lovgivning,
- og understøtter **markedets mulighed** for at levere løsninger, der kan genbruges, udbredes og konkurreres om på rimelige vilkår.

2. Behov for teknologineutralitet og fremtidssikring

Lovforslaget er udformet specifikt omkring "AI-systemer" og henviser til en dynamisk forståelse af begrebet i takt med den teknologiske udvikling.

DI vurderer dog, at selve afgrænsningen til "AI-systemer" kan medføre en uhensigtsmæssig klassifikationsøvelse: løsninger med samme funktion og samme databeskyttelsesretlige risikoprofil kan falde uden for hjemlen, hvis de ikke rubriceres som "AI", eller hvis de er hybride digitale værktøjer.

DI anbefaler derfor, at hjemlen enten:

- udvides til en mere **teknologineutral** ramme (fx "digitale beslutnings- og arbejdsgangsstøttesystemer" eller "digitale værktøjer til støtte for opgaveløsning"), eller
- som minimum suppleres med en tydelig lovteknisk mekanisme, der sikrer, at hjemlen også omfatter **funktionelt tilsvarende digitale løsninger**.

Dette vil øge retssikkerheden, reducere byrder og styrke markedets mulighed for at levere skalerbare løsninger.

3. Afgrænsningen til beslutningsstøtte bør gøres mere operationel

Lovforslaget præciserer, at ordningen ikke omfatter tilfælde, hvor afgørelser eller tiltag træffes automatisk og udelukkende på grundlag af et AI-systems output uden menneskelig involvering, herunder eftersyn og kontrol.

Samtidig fremgår det, at graden af nødvendig menneskelig involvering ikke er fastlagt klart i retspraksis.
DI forstår det bærende hensyn om, at afgørelser fortsat skal bero på en individuel og konkret vurdering, men bemærker, at uklarhed om grænsen mellem beslutningsstøtte og automatiseret sagsbehandling i praksis kan fastholde den barriere, lovforslaget netop ønsker at fjerne.

DI anbefaler, at der i forarbejderne – og gerne gennem efterfølgende national vejledning – gives konkrete typetilfælde og minimumskrav til "menneskelig involvering" for centrale anvendelser (fx

udkast til afgørelser, prioritering/triage, risikoscorer, kvalitetstjek, udkast til breve mv.), så myndigheder og leverandører får et klart, fælles udgangspunkt.

4. Opmærksomhed på fragmentering ved ressortfastsatte foranstaltninger og undtagelser

Lovforslaget lægger op til, at ressortministeren i relevant omfang kan fastsætte specifikke foranstaltninger (bl.a. i situationer med artikel 9/10-oplysninger) samt regler om undtagelse til registreredes rettigheder efter art. 23.

DI forstår, at en differentieret tilgang kan være nødvendig, men gør opmærksom på at lovforslaget i sin natur vil skabe fragmentering ved at overlade ansvaret for vurdering af konkrete foranstaltninger i medfør af § 3, stk. 2 til ressortområderne. En sådan fragmentering risikerer at skabe høje omkostninger for både myndigheder og leverandører i markedet, hvilket svækker udbredelse af relevante teknologiske løsninger og konkurrencen. DI anbefaler derfor et **fælles national katalog** (kravkatalog/skabeloner) af foranstaltninger, dokumentation og governance til beskyttelse af registreredes rettigheder, som ressortregler som udgangspunkt fastlægges ud fra. Dette sikrer mest mulig ensartethed og fleksibilitet.

I et sådan katalog bør kendte risici desuden berøres. I lovforslaget nævnes eksempelvis bias som en risiko, der bør adresseres. Andre type-risici kan med fordel adresseres med henvisninger til specifikke supplerende foranstaltninger, der kan adressere risiciene.

5. Lovforslaget løser ikke andre centrale datadelingsbarrierer
Det fremgår, at lovforslaget ikke adresserer generelle problemstillinger om videregivelse mellem myndigheder, samkøring eller tredjelandsoverførsler mv.

DI finder det relevant at anerkende denne afgrænsning, men påpeger samtidig, at netop disse problemstillinger ofte er udslagsgivende for, om løsninger kan udvikles og skaleres. I visse tilfælde - og særligt ved udvikling af AI-løsninger - vil en leverandør anses som selvstændig dataansvarlig. Dermed kræves der hjemmel til videregivelse; en problemstilling lovforslaget ikke adresserer. DI anbefaler, at der parallelt arbejdes for afklaring og harmonisering af rammerne for dataadgang og ansvar, så den nye hjemmel ikke bliver en "halv løsning" i praksis.

DI understreger desuden, at output fra trænede AI-modeller, eller videreudviklet AI-systemer langt fra altid vil udgøre personoplysninger. I sådanne tilfælde bør det være muligt for sammenslutninger af offentlige organer at benytte en model, der er trænet på personoplysninger fra forskellige offentlige kunder, uden at der er tale om videregivelse i databeskyttelsesforordningens forstand. DI skal understrege den praktiske væsentlighed i denne pointe, som delvist er nævnt på s. 16 i lovforslaget, dog alene for oplysninger der *inden* anvendelse i træningsdatasættet er *anonyme*. Denne pointe vil kunne indgå i mange sammenhænge for AI-modeller eller videreudviklede AI-systemer, hvor træningsdata har været

pseudonyme for den dataansvarlige, men *outputtet* vil være *anonymt*, da træningen alene ændrer i modellens matematiske vægtning.

Lovforslaget mangler desuden at adressere kernen i Chromebook-problematikken, da der ikke i lovforslaget er taget højde for om leverandører kan behandle data fra brugeradfærd til at forbedre servicen.

Bemærkninger til lovforslagets enkelte bestemmelser (udvalgte)
Til § 3 (udvikling og anvendelse af AI-systemer ved behandling af personoplysninger)
DI støtter formålet om at skabe et supplerende nationalt retsgrundlag, som gør det muligt at behandle personoplysninger ved brug af AI-systemer til bl.a. beslutningsstøtte, herunder udkast til afgørelser og udkast til skriftlige produkter.

DI anbefaler følgende justeringer/tilføjelser:

1. **Teknologineutralitet:** DI anbefaler, at bestemmelsen udvides eller præciseres, så den ikke alene knytter sig til "AI-systemer", men også omfatter funktionelt tilsvarende digitale løsninger, der anvendes til samme formål og under samme databeskyttelsesretlige hensyn.
2. **Klarere ramme for beslutningsstøtte:** DI anbefaler, at der i forarbejderne indsættes en mere operationel afgrænsning, så det tydeliggøres, hvornår der er tale om "beslutningsstøtte" med menneskelig involvering, og hvornår noget nærmer sig automatiseret afgørelse efter GDPR art. 22.
3. **Etablering af en entydig hjemmel:** Ordlyden af § 3, begrænser hjemlen til at understøtte "myndighedens eller organets opgavevaretagelse efter anden lovgivning". Bemærkningerne til bestemmelsen anfører, at dette vil omfatte "alle de aktiviteter, som er omfattet af de allerede fastlagte og afgrænsede regler i sektorlovgivningen, som offentlige myndigheder og organer udfører deres opgaver med hjemmel i. Opgavevaretagelsen vil både kunne omfatte afgørelser og væsentlige tiltag, men også anden forvaltningsvirksomhed og sagsbehandling, der ikke sker med henblik på at træffe en afgørelse eller iværksætte et væsentligt tiltag overfor de registrerede."

   Bestemmelsens ordlyd antages på denne baggrund at bero på en antagelse om, at al relevant anvendelse af personoplysninger, der behandles det offentlige i et AI-system vil vedrøre opgavevaretagelse (et behandlingsformål), der er fastsat i lovgivningen. Dette er med sikkerhed tilfældet ift. f.eks. en særmyndigheds adgang til at behandle personoplysninger for at træffe afgørelser, føre tilsyn mv. Men i de tilfælde, hvor anvendelse af AI ikke vedrører en borgerrettet ydelse eller en anden opgave, der er nærmere reguleret i lovgivningen, f.eks. hvis myndigheden vil benytte AI til at sikre en mere effektiv økonomiforvaltning, optimere sine it-systemer eller sagsbehandlingsprocesser eller generere ledelsesinformation mv., vil det ofte ikke være tilfældet, at disse opgaver (formål) følger af "anden lovgivning".

Endvidere er der i dag mange sammenhænge, hvor myndigheder genanvender personoplysninger, f.eks. med henblik på at varetage saglige administrative hensyn mv., der i dag ikke finder sted på baggrund af udtrykkelige hjemler i lovgivningen, men sker efter en såkaldt "forenelighedsvurdering", jf. GDPR artikel 6, stk. 4, jf. artikel 5, stk. 1, litra b. Det står DI uklart, om det er hensigten, at denne type behandlinger skal anses for omfattet af "opgavevaretagelse efter anden lovgivning" eller om det er hensigten, at understøttelse af sådanne behandlinger gennem brug af AI, ikke skal kunne finde sted efter lovforslaget. DI bemærker, at dette udgør et særskilt spørgsmål i forhold til dét, der behandles i lovforslagets punkt 2.2.3. om lovforslagets etablering af et grundlag for viderebehandling af personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 4. Formuleringen "myndighedens eller organets opgavevaretagelse efter anden lovgivning" i lovforslagets § 3 ses således – muligvis utilsigtet – at opretholde den grundlæggende hjemmelsusikkerhed på området i forhold til behandlinger af personoplysninger, der i dag ikke hviler på fastlagte og afgrænsede regler i sektorlovgivningen.

DI bemærker i den forbindelse, at en meget væsentlig del af potentialet ved AI, må formodes at knytte sig til optimering af den offentlige sektors drift og ikke kun ifm. egentlig afgørelsesvirksomhed, beslutningsstøtte eller anden forvaltningsvirksomhed, der udøves i henhold til lov eller regler fastsat i medfør af lov (bekendtgørelser). Sådanne anvendelser af AI vil også ofte omfatte behandling af personoplysninger om borgere såvel som medarbejdere, men ikke – som forudsat i bemærkningerne – hvile på "allerede fastlagte og afgrænsede regler i sektorlovgivningen", der angiver en mere effektiv drift som et databeskyttelsesretlig behandlingsformål, som myndigheden skal varetage. Der ses derfor at være en væsentlig risiko for, at hensigtsmæssige, legitime og ønskværdige AI-projekter, der alene har til formål at effektivisere og forbedre driften af den offentlige sektor, i databeskyttelsesretlig forstand, ikke kan anses for hjemlet i lovforslagets § 3. Det anbefales derfor, at det helt udtrykkeligt anføres i § 3, at myndigheder også kan anvende AI til at varetage "en mere effektiv drift" eller lignende. Netop hensynet til at gøre den offentlige sektor mere effektiv, ses også at være nævnt i lovforslagets indledning som del af motivationen for lovforslaget. Fastsættelsen af dette behandlingsformål, der som nævnt allerede i dag varetages lovligt af myndigheder på et ikke nærmere lovreguleret grundlag, må generelt anses som ét formål, der lovligt kan varetages inden for rammerne af GDPR.

4. **Adgang til at regulere dataansvar, opbevaringsperioder mv.**: Som anført i lovforslagets punkt 2.2.1.1.1. kan medlemsstater efter GDPR artikel 6, stk. 3, fastsætte et supplerende retsgrundlag efter databeskyttelsesforordningen, der kan indeholde specifikke bestemmelser med henblik på at tilpasse anvendelsen af bestemmelserne i databeskyttelsesforordningen, bl.a. de generelle betingelser for lovlighed af den dataansvarliges behandling, hvilke typer oplysninger der skal behandles, berørte registrerede, hvilke enheder personoplysninger må videregives til, og formålet hermed, formålsbegrænsninger, opbevaringsperioder og behandlingsaktiviteter samt behandlingsprocedurer, herunder foranstaltninger

til sikring af lovlig og rimelig behandling såsom i andre specifikke databehandlingssituationer. EU-retten eller medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, der forfølges.

DI vurderer, at der som led i udvikling og anvendelsen af AI-løsningen i det offentlige vil kunne opstå en række – ofte komplekse – spørgsmål knyttet til denne type af forhold. F.eks. kan spørgsmålet om hvilke myndigheder, der skal være dataansvarlige for udviklingen eller driften af en AI-løsning ofte opstå, hvis f.eks. en række kommuner eller regioner samarbejder om en fælles udvikling af et AI-værktøj. Det vil i den forbindelse være en byrdelettelse og sikre de mest betryggende databeskyttelsesretlige rammer, såfremt en entydig forankring af dataansvaret – og dermed f.eks. hvilken myndighed, der er ansvarlig for dokumentation, udarbejdelse af DPIA mv. – kan fastsættes ved bekendtgørelse fremfor at bero på en fælles fortolkning af definitionerne i GDPR. Endvidere kan der i konkrete AI-projekter opstå spørgsmål om hvilke sletteregler, der skal gælde for behandlede personoplysninger, hvilke sikkerhedskrav, der bør iagttages, om der bør anvendes anonymisering eller pseudonymisering i faser af et projekt mv.

Og som også afspejlet i Digitaliseringsstyrelsen evaluering af AI-signaturprojekterne efterspørger bl.a. kommuner i vidt omfang klarere rammer for, hvordan den praktiske afvikling af AI-projekter skal finde sted i lyset af de juridiske krav, der følger af GDPR. Kravene i GDPR fortolkes således forskelligt på tværs af myndigheder eller er uklare.

DI skal derfor opfordre til, at lovforslaget udvides til også at omfatte en adgang for den relevante ressortminister til – efter behov og hvor relevant og efter forudgående høring af Datatilsynet – at regulere forhold omfattet af GDPR artikel 6, stk. 3, ved bekendtgørelse.

5. **Fælles katalog for "specifikke foranstaltninger":** Lovforslagets § 3, stk. 2 vil medføre, at der på tværs af ressortområder vil eksistere krav om "specifikke foranstaltninger" med henblik på at efterleve de særskilte krav der kan være hertil i databeskyttelsesforordningens artikel 9, stk. 2. DI anbefaler, at bemærkningerne til lovforslaget indeholder et ikke-udtømmende katalog af foranstaltninger til beskyttelse af den registreredes rettigheder . Hensigten er, så vidt muligt, at ensarte passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser i forbindelse med behandling omfattet af stk. 1, når behandlingen omfatter personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10.**Implementering af specifikke foranstaltninger på ressortområderne skal styres af en tværgående enhed:** DI anbefaler, at arbejdet med identifikation af nødvendige supplerende sektorregler og implementering af sådanne styres af en tværgående enhed, der nedsættes i myndighedsregi. Enheden skal sikre, at
    1. Behovet for brug af nye teknologier, herunder AI, til behandling af særlige kategorier af personoplysninger og personoplysninger om straffedomme og lovovertrædelser i de enkelte sektorer afdækkes.

2. Det identificeres i hvilke sektorlovgivninger supplerende foranstaltninger er nødvendige **og** bemyndigelsen i § 3, stk. 2 til at iværksætte passende og specifikke foranstaltninger udnyttes.
3. De iværksatte passende og specifikke foranstaltninger så vidt muligt dækker sektorbehovet bredt og ikke blot enkelte use-cases, som anført af ministeriet på s. 45.
4. Hvert ressortministerium inden for en fastsat frist tager stilling til, om eksisterende sektorlovgivning og beskyttelsesforanstaltninger er tilstrækkelige til udvikling og anvendelse af AI-systemer, eller om der er behov for supplerende lovgivning eller regler i medfør af § 3, stk. 2
5. Resultatet af gennemgangen samles i en fælles, offentlig oversigt, som løbende opdateres, og som også tydeligt angiver de områder, hvor eksisterende regulering vurderes tilstrækkelig, så myndigheder ikke afventer nye regler, hvor sådanne ikke er nødvendige
6. Der efter en fast periode følges op på, om sektorlovgivning, datadeling eller manglende supplerende foranstaltninger fortsat udgør barrierer for udvikling og skalering af AI-systemer i den offentlige sektor.

For så vidt angår lovforslagets § 3, stk. 2, hvorefter ressortmyndighederne skal fastlægge specifikke foranstaltninger, noterer DI sig at det af lovbemærkningerne på s. 45 fremgår at *''der efter bestemmelsen kan fastsættes nærmere regler, indebærer ikke, at der i hvert tilfælde skal fastsættes regler [DI understregning]. Det vil således – ud fra en konkret vurdering – kunne besluttes, at de krav, der eventuelt følger af anden gældende ret, er tilstrækkelige foranstaltninger.''*

DI forstår lovbemærkningen sådan, at der kan fastsættes specifikke foranstaltninger, hvor der vil ske behandle af særlige kategorier af personoplysninger og oplysninger om straffedomme og lovovertrædelser, men at bemyndigelsesbestemmelsen ikke altid medfører, at dette skal være tilfældet. DI bifalder ministeriets overvejelser, men understreger at den blotte tilstedeværelse af en bemyndigelsesbestemmelse allerede skaber usikkerhed om særligt kommunernes og regionernes villighed til at vurdere, at allerede fastsatte foranstaltninger er tilstrækkelige. DI håber derfor, at ministeriet vil indsætte eksempler på sektorlovgivning, hvor foranstaltninger enten allerede er fastlagt eller er ved at blive det.

Til § 4 (undtagelse til registreredes rettigheder)

DI forstår bestemmelsen sådan, at den udgør en bemyndigelse for det relevante ressortområde, der vil bruge AI i deres opgavevaretagelse, til at fravige databeskyttelsesreglernes krav om registreredes rettigheder.

DI er enige i at dette udgør et væsentligt værn for retten til privatliv og forstår at der ikke kan fastlægges en generel undtagelse. DI noterer sig dog – og er i visse tilfælde enig i - de grundlæggende udfordringer mellem kravene til registreredes rettigheder og teknologiens natur, og påpeger, at der bør anlægges en pragmatisk tilgang til håndhævelse. Det kan eksempelvis være ved at sikrer de registreredes rettigheder såsom oplysningspligten, fastlægges i den lov der udmøntes via bemyndigelsesbestemmelsen, men også ved at anerkende hvornår en trænet AI-model eller et videreudviklet AI-system *ikke* udgør behandling af personoplysninger.

DI vil i sammenhæng hermed understrege, at en trænet AI-model består af matematiske vægte og derfor ikke nødvendigvis udgør personoplysninger, som er omfattet af kravene i databeskyttelsesforordningens kapitel III om registreredes rettigheder. Er personoplysningerne eksempelvis tilstrækkeligt pseudonymiseret træningen, vil outputtet fra den trænede AI-model eller det videreudviklede AI-system ikke være muligt at henføre tilbage til en bestemt fysisk person, og dermed ikke udgøre personoplysninger.

DI foreslår på den baggrund, at ministeriet opdaterer lovbemærkningernes afsnit 3.1, således at det ikke kun understreges at *''et AI-system i sin natur potentielt vil kunne medføre en begrænsning af den registreredes rettigheder''*, men at det også understreges, at selvom træningsdata i træningsøjeblikket kan udgøre pseudonyme personoplysninger for den dataansvarlige, vil det ikke medføre at AI-modellen indeholder personoplysninger, eller at det efterfølgende *output* er henførbart.

Afsluttende bemærkninger

DI støtter grundlæggende lovforslagets intention om at skabe et klart databeskyttelsesretligt retsgrundlag for myndigheders udvikling og anvendelse af AI-systemer i den offentlige sektor. For at lovforslaget bedst muligt bidrager til ansvarlig innovation, effektivisering og et velfungerende leverandørmarked, anbefaler DI, at hjemlen gøres mere teknologineutral og entydig samt at der etableres fælles, skalerbare rammer, som modvirker fragmentering på tværs af sektorer. DI anbefaler samtidig en forpligtende mekanisme for løbende at sikre, at sektorlovgivningen følger med den teknologiske udvikling og ikke bliver en utilsigtet barriere for anvendelsen af den generelle hjemmel.

DI står naturligvis til rådighed for uddybning og dialog.

Dansk Selskab for Almen Medicin

København, den 8. oktober 2026

Til Digitaliseringsstyrelsen

Høringssvar vedr. fornyet høring over udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Dansk Selskab for Almen Medicin (DSAM) takker for muligheden for at kommentere det reviderede lovforslag. DSAM var ikke på høringslisten ved den første høring, som blev afbrudt ved valgudskrivelsen, men afgav høringssvar den 2. marts 2026. DSAM kvitterer for denne gang at være på høringslisten.

Lovforslaget giver myndigheder og organer en generel, supplerende hjemmel til at behandle personoplysninger ved udvikling og anvendelse af AI som led i deres lovbestemte opgaver. Sektorlovgivningen, herunder sundhedslovgivningen, gælder fortsat. Hjemlen spænder fra rutineadministration til klinisk beslutningsstøtte med helbredsoplysninger. Dataetisk Råds formand har kritiseret dens bredde og manglende sondring mellem oplysningstyper og anvendelser, blandt andet med henvisning til forskellen mellem bibliotekslån og sundhedsoplysninger [(1)].

Lovforslaget regulerer alene databehandling. Patientbehandling er fortsat underlagt sundhedslovgivningens regler om information, samtykke, journalføring, tavshedspligt, lovbestemt datadeling og faglig forsvarlighed. Den nye hjemmel ændrer ikke i sig selv, hvad en sundhedsperson må gøre over for en patient, og § 4 giver ikke adgang til at begrænse patientens rettigheder efter sundhedslovgivningen.

AI har betydeligt potentiale i sundhedsvæsenet, og der findes allerede klinisk validerede modeller til blandt andet billeddiagnostik og risikostratificering. DSAM's bemærkninger skal ses i dette lys. Fire forhold begrunder særlige krav til brug af den nye hjemmel på sundhedsområdet:

- **Fortrolighed er afgørende for patientbehandling.** Patienter skal kunne stole på tavshedspligten, så de trygt fortæller det, der er nødvendigt for udredning og patientbehandling.

- **Fejl i helbredsoplysninger kan føre til forkert patientbehandling.** Datadeling og datagenbrug kan lade fejl følge patienten gennem mange systemer. Rettelser skal derfor slå igennem dér, hvor oplysningerne bruges, også når det gælder AI, jf. afsnit 2.1.

- **Patientens selvbestemmelse skal sikres.** Undersøgelse og patientbehandling kræver som udgangspunkt informeret samtykke. Sundhedslovgivningens patientrettigheder gælder også ved klinisk AI. Der er behov for klare regler om information og mulighed for at fravælge klinisk AI i egen udredning og patientbehandling, jf. afsnit 3.2.

- **Medicinsk AI kræver tilstrækkelig kontrol.** AI beregnet til eksempelvis medicinsk monitorering, diagnostik eller valg af patientbehandling er som udgangspunkt medicinsk udstyr med krav om CE-mærkning. EU-forordningen om medicinsk udstyr (MDR) tillader dog på nærmere betingelser sundhedsinstitutioners egen udvikling og brug uden CE-mærkning og uden krav om uafhængig forhåndsvurdering. Den nye hjemmel kan efter DSAM's vurdering øge denne brug. Kontrollens tilstrækkelighed bør derfor afklares, jf. afsnit 4.

Hjemlen bør derfor ledsages af bindende beskyttelseskrav for helbredsoplysninger, også i sundhedsinstitutioners egne systemer.

Lovforslaget har væsentlig betydning for sundhedsvæsenet. DSAM finder det derfor kritisabelt, at blandt andre Lægeforeningen, Praktiserende Lægers Organisation og Dansk Sygeplejeråd fortsat mangler på høringslisten, på trods af DSAM's kritik af samme problem ved den første høring.

DSAM's hovedanbefalinger er:

- **Bindende minimumskrav før brug.** Loven skal pålægge den ansvarlige minister at fastsætte bindende, risikotilpassede minimumskrav efter § 3, stk. 2, til AI-baseret databehandling af helbredsoplysninger. Kravene skal omfatte risikostyring, datakvalitet, tilladte oplysningskategorier, logning, menneskeligt tilsyn og dokumentation. De skal også gælde sundhedsinstitutioners egenudviklede systemer og være trådt i kraft, før den nye hjemmel bruges til helbredsoplysninger.

- **Faste rammer for rettighedsbegrænsninger.** Loven skal stille minimumskrav til bekendtgørelser efter § 4 om formål, datatyper, rækkevidde, varighed, garantier og efterprøvelse. Nødvendighed og forholdsmæssighed skal begrundes offentligt. Begrænsninger skal knyttes til afgrænsede systemer eller databehandlinger og må ikke omfatte hele sektorer. For helbredsoplysninger må § 4 ikke begrænse retten til rettelse eller indsigelse, retten til begrænsning af databehandlingen, mens en bestridt oplysnings rigtighed undersøges, eller pligten til at underrette modtagere om rettelser og begrænsninger.

- **Konsekvensanalyse og åbenhed før brug.** Loven skal kræve en dækkende, risikotilpasset konsekvensanalyse vedrørende databeskyttelse (DPIA), før hjemlen bruges til AI-baseret databehandling af personoplysninger, også uden pligt efter artikel 35 i databeskyttelsesforordningen (GDPR). Nødvendige beskyttelsesforanstaltninger og en offentlig version af analysen skal være på plads før databehandlingen. Begge versioner skal holdes ajour. Udeladelser fra den offentlige version skal begrundes konkret med angivelse af retsgrundlaget.

- **Datakvalitet og rettelser på tværs af systemer.** Loven skal sikre rammerne for tilstrækkelig datakvalitet ved al databehandling efter loven. Rettelser og afkræftelser i kildesystemerne skal slå igennem i AI-systemernes datagrundlag og data til gentræning, også efter deling eller kopiering. Borgeren og beslutningstageren skal kunne se, hvilke oplysninger systemet har lagt til grund. Fejl i den enkeltes oplysninger kan give forkerte resultater, selv om systemet fungerer godt med korrekte inputdata.

- **Værn for datasamlinger til AI.** Loven bør begrænse politiets og efterretningstjenesternes adgang til datasamlinger, der indeholder helbredsoplysninger og er opbygget efter loven til udvikling og anvendelse af AI. Oplysninger fra disse datasamlinger bør kun kunne udleveres i konkrete sager. Udlevering bør kræve en forudgående retskendelse og en begrundet, individuel mistanke mod den person, oplysningerne vedrører. Politi og efterretningstjenester bør hverken have løbende søgeadgang eller adgang til hele datasamlinger til generel efterretningsanalyse. Værnet bør omfatte hele datasamlingen og gælde på tværs af myndighedsområder. Det skyldes, at helbredsoplysninger sammenstillet med andre oplysninger kan give et mere detaljeret billede af borgeren end kildesystemerne hver for sig. Tilsvarende værn bør overvejes for andre særligt følsomme oplysninger, jf. afsnit 2.3.

- **Klare rammer for genbrug og ret til fravalg.** Viderebehandling af helbredsoplysninger til udvikling og gentræning efter loven skal kræve en konkret vurdering af foreneligheden med det oprindelige formål. Fastholdes adgangen uden en sådan vurdering, skal lovhjemlens nødvendighed og forholdsmæssighed begrundes, og hvert projekts formål og datakategorier afgrænses med dokumenteret nødvendighed, forholdsmæssighed og dataminimering. Patienter bør kunne fravælge brug af deres helbredsoplysninger til udvikling og gentræning efter loven, uanset om formålet beskrives som patientbehandling, kvalitetsudvikling eller forskning. De bør også kunne fravælge klinisk AI i egen udredning og patientbehandling, så sundhedspersonens vurdering foretages uden støtte i AI-forslag.

- **Kontrol med egenudviklet medicinsk AI.** Lovbehandlingen skal undersøge, om hjemlen kan øge brugen af egenudviklet medicinsk AI uden CE-mærkning under MDR artikel 5, stk. 5 (in-house-undtagelsen). Behovet for supplerende patientsikkerhedskontrol og lovgrundlaget herfor skal afklares. DSAM foreslår inden for EU-rettens rammer CE-mærkning af nærmere afgrænsede typer medicinsk AI ved betydelig klinisk risiko eller bred anvendelse. Systemer, der fortsat bruges under undtagelsen, bør vurderes uafhængigt før brug, jf. afsnit 4.

De uddybende kommentarer følger nedenfor. Afsnit 1 og 2 vedrører databehandling og borgerrettigheder med særlig vægt på helbredsoplysninger. Afsnit 3 og 4 vedrører klinisk anvendelse, patientens selvbestemmelse og medicinsk AI. Sidehenvisninger gælder lovudkastets bemærkninger.

1. Retssikkerhedsmæssige hovedpunkter

Lovforslaget giver ministrene mulighed for at fastsætte bindende beskyttelseskrav efter § 3, stk. 2, og begrænse visse GDPR-rettigheder efter § 4. DSAM ønsker tydeligere rammer og minimumskrav i selve loven.

1.1 Bindende garantier, økonomi og grænser for rettighedsbegrænsninger

Bindende minimumskrav skal være en pligt

I § 3, stk. 2, er det første udkasts »skal« ændret til »kan«, og bemærkningerne afviser en generel pligt til at fastsætte beskyttelsesforanstaltninger (s. 32). Pligten består dog, når databeskyttelsesreglerne kræver sådanne foranstaltninger (s. 50). Datatilsynet lagde ved den første høring til grund, at nødvendige yderligere foranstaltninger i disse tilfælde skal være fastsat ved bekendtgørelse, før oplysningerne behandles [(2)]. DSAM anbefaler mere generelt en udtrykkelig lovfæstet pligt til fælles, bindende minimumskrav, før hjemlen bruges til helbredsoplysninger.

Uden fælles krav må den enkelte dataansvarlige, eksempelvis en region, kommune eller lægepraksis, i højere grad selv fastlægge og begrunde kontrolniveauet, jf. afsnit 3.1. Det kan give dobbeltarbejde og forskelle i patientbeskyttelsen. For systemer på tværs af ministerområder, eksempelvis i den kommunale ældrepleje, åbner bemærkningerne for fælles bekendtgørelser (s. 75). Udkastet stiller dog hverken krav om fælles regler eller en generel frist for udstedelsen af bekendtgørelser. Dataetisk Råd anbefalede ved den første høring generelle minimumskrav til beskyttelse af følsomme oplysninger på tværs af ministerområder, som de enkelte ministre kun skal supplere, hvor det er nødvendigt [(3)]. Et centralt fastsat minimumsniveau bør gælde alle, der behandler helbredsoplysninger efter loven, og bør også overvejes på andre områder.

Sundhedsområdet har allerede egne regler om beslutningsstøtte

Ved lov nr. 717 af 20. juni 2025 blev der vedtaget en ny § 48 e i sundhedsloven om blandt andet databehandling af helbredsoplysninger til beslutningsstøtte ved patientbehandling, herunder oplysninger tidligere behandlet til forskning og statistik. Stk. 3 pålægger ministeren at fastsætte nærmere regler: Ordlyden er »fastsætter«, mens lovudkastets § 3, stk. 2, bruger »kan« [(4)]. Ministeren bestemmer også ikrafttrædelsestidspunktet (lovens § 4, stk. 2). En bekendtgørelse har været i høring, og DSAM afgav høringssvar den 14. januar 2026 [(5)]. Så vidt DSAM er bekendt, er den endnu ikke udstedt. Allerede i 2019 fik ministeren desuden bemyndigelse til at regulere autoriserede sundhedspersoners indhentning af oplysninger om den aktuelle patient og andre patienter til beslutningsstøtte ved patientbehandling (sundhedslovens § 42 a, stk. 7).

AI-hjemmelsloven skal gælde sideløbende med sektorlovgivningen. Bemærkningerne åbner dog for, at ministrene ved senere revisioner kan overveje at lade AI-anvendelse ske med hjemmel i den nye lov (s. 15–16). Samtidig kan sektorregler eller den dataansvarliges egne retningslinjer mindske behovet for yderligere beskyttelseskrav efter § 3, stk. 2 (s. 31 og 73). Samspillet med sundhedslovens § 48 e og reglerne efter bestemmelsen bør derfor afklares under lovbehandlingen.

Rammerne for begrænsninger efter § 4 bør stå i loven

Ifølge bemærkningerne kan begrænsninger efter § 4 omfatte hele sektorer eller enkelte AI-systemer (s. 41). § 4, 2. pkt. gengiver desuden fortsat GDPR artikel 23, stk. 2, uden forordningens ord »som minimum«. DSAM påpegede ved den første høring, at udeladelsen signalerer et svagere kravniveau end forordningen forudsætter, og ordene bør indsættes i lovteksten. Datatilsynet har vurderet, at generelle undtagelser for grupper af dataansvarlige næppe er forenelige med GDPR, og fundet det ikke indlysende, at bekendtgørelser fra samtlige ressortministre kan sikre den klarhed, GDPR artikel 23 kræver [2]. Institut for Menneskerettigheder anbefalede ved den første høring, at betingelserne og garantierne for rettighedsbegrænsninger præciseres yderligere i lovforslaget [6]. Dataetisk Råd anbefalede tilsvarende, at selve lovteksten fastslår, at undtagelser skal være nødvendige og proportionale, angiver deres mulige karakter og præciserer de rettigheder og situationer, hvor ministrene ikke kan gøre undtagelse [3]. DSAM anbefaler, at de står i selve lovteksten, og at begrænsninger knyttes til afgrænsede systemer eller databehandlinger, aldrig til hele sektorer, jf. afsnit 2.2. Afgrænsning til et bestemt system eller en bestemt databehandling er ikke i sig selv tilstrækkelig, idet også de berørte personer, rettigheder og situationer skal afgrænses efter nødvendighed og forholdsmæssighed.

DSAM finder det positivt, at Datatilsynet skal høres, før der fastsættes regler efter både § 3, stk. 2, og § 4 (s. 75 og 79).

Udgifterne til databeskyttelse bør indgå i den økonomiske vurdering

Lovudkastet omtaler effektiviseringsgevinster og udgifter til anskaffelse, implementering, oplæring og vedligeholdelse, men belyser ikke særskilt risikovurdering, konsekvensanalyse, logning, stikprøver og tilsyn. Bekendtgørelsernes økonomiske konsekvenser vurderes først ved udstedelsen (s. 48–49). Datatilsynet efterlyste allerede ved den første høring, at arbejdet med at overholde databeskyttelsesreglerne indgår i vurderingen af ressourcebehovet [2]. En uafhængig it-sikkerhedsrådgiver anslår, at den løbende kontrol og dokumentation kan koste 10 til 20 procent af et systems anskaffelsespris om året [7].

Udkastet begrunder fraværet af udgifter som følge af nye pligter med, at ingen pålægges at bruge hjemlen (s. 48). Gevinsterne forudsætter imidlertid, at den bruges, og dermed også udgifter til kontrol og dokumentation hos regioner, kommuner og lægepraksisser. En uafhængig it-rådgiver har med henvisning til DUT-princippet peget på, at regningen ikke forsvinder, fordi anvendelsen kaldes frivillig, men flytter til de kommunale budgetter [8]. Både gevinsterne og de nødvendige udgifter bør indgå i lovforslagets økonomiske vurdering.

DSAM anbefaler:

- **at loven pålægger den ansvarlige minister at fastsætte fælles, bindende minimumskrav til AI-baseret databehandling af helbredsoplysninger. Kravene skal være trådt i kraft, før den nye hjemmel bruges til helbredsoplysninger, også til udvikling og gentræning af AI-systemer.**

- **at loven konkretiserer GDPR's rammer for rettighedsbegrænsninger efter § 4 gennem krav til formål, datatyper, rækkevidde, varighed, garantier og efterprøvelse.**

Hver bekendtgørelse skal ledsages af en offentlig begrundelse for nødvendighed og forholdsmæssighed, herunder hvorfor mindre indgribende løsninger ikke er tilstrækkelige. Begrænsninger skal knyttes til afgrænsede systemer eller databehandlinger og må ikke omfatte hele sektorer.

- **at loven afklarer samspillet med sundhedslovens § 48 e ved udvikling og brug af klinisk beslutningsstøtte. Det skal fremgå, hvilke krav der gælder ved overlap, og at den nye hjemmel ikke giver adgang til at fravige sundhedslovgivningens beskyttelseskrav.**

1.2 Dokumentation og efterprøvelighed

Minimumskravene bør sikre, at AI's bidrag til kliniske beslutninger kan efterprøves. DSAM anbefaler automatisk logning af systemets inputoplysninger, svar, tidspunkt og modelversion, da opdateringer og gentræning kan ændre svar og anbefalinger.

Logningen bør ske uden manuel registrering fra sundhedspersonen og uden unødig kopiering eller opbevaring af helbredsoplysninger. Entydige referencer kan erstatte kopier, hvis det faktisk anvendte datagrundlag kan genskabes enkelt og med små omkostninger.

Reel menneskelig vurdering kræver bindende procedurer

Logning dokumenterer systemets bidrag, men ikke i sig selv sundhedspersonens selvstændige vurdering. Den skal derfor suppleres med bindende procedurer for reel menneskelig vurdering, jf. afsnit 3.1.

Dokumentationen er også nødvendig ved tilsyn og klagebehandling. Folketingets Ombudsmand oplyste den 18. august 2026, at den havde bedt en række kommuner redegøre for blandt andet vejledningspligt, notatpligt og saglighed ved AI-brug [9]. På sundhedsområdet skal Styrelsen for Patientsikkerhed, Styrelsen for Patientklager og Datatilsynet tilsvarende, inden for deres respektive opgaver, kunne sammenholde systemets anbefaling og datagrundlag med sundhedspersonens dokumenterede beslutning.

AI-forordningens logningskrav dækker ikke alle kliniske systemer

AI-forordningen kræver automatisk registrering af relevante hændelser i højrisikosystemer [10]. Det gælder blandt andet medicinsk AI-udstyr, der kræver vurdering ved et bemyndiget organ. Efter ændringsforordningen fra 2026 gælder højrisikokravene først fra 2. december 2027 eller 2. august 2028, afhængigt af klassifikationen, og med overgangsregler for allerede ibrugtagne systemer [11]. Internt fremstillede medicinske AI-systemer kan også derefter falde uden for højrisikoklassifikationen, jf. afsnit 4.

Logning af klinisk AI-beslutningsstøtte med helbredsoplysninger bør derfor være bindende efter loven, uanset højrisikoklassifikation og før AI-forordningens højrisikokrav gælder.

Logning og journalføring supplerer hinanden

Logning erstatter ikke journalføring, jf. afsnit 3.1. Journalføringsreglerne gælder også ved AI-brug, men indeholder ikke særskilte krav om AI-baseret beslutningsstøtte [12]. Behovet for præcisering eller supplering bør afklares.

Loggen bør bevare den oprindelige registrering og opbevares mindst lige så længe som journalen, når den er nødvendig for at forstå journalnotatet. AI-forordningen kræver, at logs fra højrisikosystemer opbevares i en periode, der passer til formålet, og som udgangspunkt mindst seks måneder, jf. forordningens artikel 26, stk. 6 [10]. Seks måneder er efter DSAM's opfattelse ikke tilstrækkeligt, når loggen er nødvendig som klinisk dokumentation. Loggen bør i så fald indgå i journalen.

Patienters adgang til egen log

Patienten bør kunne se brugen af egne helbredsoplysninger, også til udvikling, træning og gentræning. DSAM foreslår adgang med MitID til en oversigt over, hvilke oplysninger der er brugt i hvilke AI-systemer eller projekter, hvornår, til hvilke formål, og hvem der er dataansvarlig. Patienten bør kunne anmode om rettelse samme sted, jf. afsnit 2.1 og 2.2.

Min Log på sundhed.dk kan inspirere løsningen. Det bør undersøges, hvordan eksisterende løsninger kan udbygges til at dække både klinisk brug og udviklings- og træningsprojekter. Erfaringerne kan senere bruges på andre myndighedsområder, jf. afsnit 2.3.

DSAM anbefaler:

- **at bekendtgørelser efter § 3, stk. 2, kræver automatisk logning ved AI-baseret klinisk beslutningsstøtte med helbredsoplysninger efter loven. Loggen skal omfatte datagrundlag, svar, tidspunkt og algoritme- eller modelversion. Entydige referencer kan erstatte datakopier, hvis grundlaget kan genskabes. Logningen skal ske uden manuel registrering fra sundhedspersonen og med begrundede opbevaringsfrister. Kravene skal tilpasses risikoen med udgangspunkt i AI-forordningens relevante højrisikokrav, også uden for højrisikoklassifikationen.**

- **at patienterne får adgang til en oversigt over brugen af egne helbredsoplysninger i AI-systemer og udviklings- og træningsprojekter.**

1.3 Konsekvensanalyse og offentlighed

GDPR artikel 35 kræver en konsekvensanalyse vedrørende databeskyttelse (DPIA) før databehandling, der sandsynligvis indebærer høj risiko for de registreredes rettigheder og frihedsrettigheder. De europæiske databeskyttelsesmyndigheders retningslinjer understreger behovet for løbende revurdering og fremhæver offentliggørelse af analysen eller et resumé som god praksis for offentlige myndigheder. Offentliggørelse er dog ikke et krav [13].

DSAM anbefaler en obligatorisk analyse og offentlig version ved brug af den nye hjemmel, også uden høj risiko. Ved enkel databehandling med begrænset risiko kan analysen være tilsvarende enkel. Institut for Menneskerettigheder anbefalede ved den første høring, at myndigheder som klart udgangspunkt skal udarbejde og offentliggøre menneskeretlige konsekvensanalyser før ibrugtagning af AI [6]. Vurderingerne kan samles, hvis analysen både opfylder DPIA-kravene og dækker de menneskeretlige konsekvenser, herunder risikoen for forskelsbehandling. Dataetisk Råd anbefalede ved den første høring desuden en samlet dataetisk konsekvensanalyse af selve lovforslaget [3].

DSAM støtter dette, og de enkelte projekters analyser bør suppleres af en samlet vurdering af lovens følger for fortrolighed, ligebehandling og frihedsrettigheder.

DSAM anbefaler:

- **at loven kræver en dækkende, ajourført DPIA, før personoplysninger behandles til AI-udvikling eller -anvendelse efter den nye hjemmel, også uden pligt efter GDPR artikel 35. Omfanget skal afspejle databehandlingens karakter, omfang og risici. Analysen skal beskrive tidspunktet for og omfanget af menneskelig medvirken i beslutningerne. Nødvendige beskyttelsesforanstaltninger skal være iværksat før databehandlingen, og analysen skal opdateres ved ændringer, der kan påvirke risikoen for de registrerede.**

- **at en offentlig version skal foreligge før databehandlingen og holdes ajour. Den skal beskrive nødvendighed, forholdsmæssighed, risici, beskyttelsesforanstaltninger og samlede konklusioner. Udeladelser, eksempelvis af hensyn til personers rettigheder eller informationssikkerhed, skal begrundes konkret med angivelse af retsgrundlaget i den offentlige version.**

2. Rettigheder og databeskyttelse

2.1 Helbredsoplysninger, fejl og datakvalitet

Databehandling af helbredsoplysninger kræver både et retsgrundlag efter GDPR artikel 6 og en undtagelse efter artikel 9, stk. 2, fra forbuddet i artikel 9, stk. 1, mod databehandling af følsomme oplysninger. Beskyttelsen skal afspejle formål, omfang og risiko. Efter Datatilsynets praksis kan indgribende AI-baseret databehandling stille skærpede krav til hjemlens klarhed (s. 22 og 27). AI kan også udlede følsomme oplysninger af data, som hver for sig ikke er følsomme (s. 74). Beskyttelsen skal derfor omfatte både de indgående og de udledte følsomme oplysninger.

DSAM er enig i bemærkningernes præcisering af, at AI ikke i sig selv er en væsentlig samfundsinteresse, der kan begrunde databehandling af helbredsoplysninger (s. 72). Samtidig beskrives loven som et supplerende retsgrundlag efter GDPR artikel 9, stk. 2 (s. 44). Det bør derfor præciseres, hvad loven hjemler efter artikel 9, stk. 2, litra g, og hvilke betingelser der fortsat skal opfyldes efter databeskyttelsesreglerne og sundhedslovgivningen, især ved udvikling og gentræning. Anvendes undtagelsen for sundhedsformål i artikel 9, stk. 2, litra h, skal tavshedspligtskravet i artikel 9, stk. 3, også være opfyldt.

Fejl i sundhedsdata kan være hyppige

Fejl i helbredsoplysninger er veldokumenterede, også i danske registre og journalsystemer [14]. I en undersøgelse af Det Nationale Diabetesregister var 21 procent af den undersøgte population identificeret alene ud fra hyppigheden af blodsukkermålinger uden krav om værdier over diagnosegrænsen [15]. Det er ikke i sig selv en fejlprocent, men viser usikkerheden ved registreringsgrundlaget. En gennemgang i én lægepraksis viste desuden, at 10–15 procent af de patienter, der var registreret med type 2-diabetes, var fejldiagnosticerede [16].

I en international undersøgelse havde omkring 60 procent af personer med oplyst lægediagnosticeret KOL, kronisk bronkitis eller emfysem ikke luftvejsobstruktion ved spirometri [17]. I en dansk familieundersøgelse af medfødt hjertesygdom var 36 procent af de undersøgte patienter fejlklassificerede i registret [18].

Undersøgelserne belyser forskellige problemer, men viser, at registrerede helbredsoplysninger ikke nødvendigvis er korrekte. Det ændres ikke, når oplysningerne bruges af AI.

Fejl i inputdata kan ramme samme patient gentagne gange

Et AI-system kan fungere godt på gruppeniveau og alligevel give gentagne forkerte vurderinger af en patient på grund af en fejlagtig diagnose eller et forkert fund. Når oplysninger deles mellem journaler, registre og andre systemer, kan fejlen følge patienten i årevis og påvirke risikovurdering, prioritering og patientbehandling. En rettelse ét sted er derfor ikke altid nok.

Journaloplysninger kan rettes eller suppleres, men den oprindelige registrering skal bevares. AI-systemer skal derfor kunne skelne den fra senere rettelser, afkræftelser og forbehold. En afkræftet diagnose kan være relevant som sygehistorie, men må ikke bruges som gældende diagnose. Rettelserne skal også følge med til data til gentræning, så allerede erkendte fejl ikke videreføres.

Rettelser skal slå igennem på tværs af systemer

GDPR kræver allerede korrekte og om nødvendigt ajourførte personoplysninger. Datatilsynet fremhævede dette som centralt ved AI i den første høring [2]. Efter GDPR artikel 19 skal modtagere som udgangspunkt underrettes om rettelser. Bestrider en person en oplysnings rigtighed, giver GDPR artikel 18 ret til begrænsning af databehandlingen, mens rigtigheden undersøges.

Rettighederne skal også fungere i AI-systemer. Undtagelser fra underretningspligten må ikke blive hovedreglen. Systemerne bør indrettes, så alvorlige fejl kan markeres, korrigeres eller blokeres på tværs af de systemer, oplysningerne er delt med.

Datakvalitet bør være et fælles minimumskrav

AI-forordningen stiller særlige krav til højrisikosystemers trænings-, validerings- og testdata. Den anvendende organisation skal desuden sikre relevante og tilstrækkeligt repræsentative inputdata, i det omfang den har kontrol over dem [10].

Minimumskravene efter § 3, stk. 2, bør omfatte datakvalitet, rettelser, afkræftelser og ajourføring, også uden for højrisikoklassifikationen. Sundhedspersonen og patienten bør tillige kunne se, hvilke oplysninger systemet har lagt til grund, jf. afsnit 1.2 og 2.2.

Erfaringer fra andre digitale systemer

Problemerne findes også uden for sundhedsvæsenet. De danske ejendomsvurderinger bygger på registerdata, hvor fejl kan påvirke den enkelte ejers vurdering. For oplysninger i Bygnings- og Boligregistret (BBR) har ejeren selv pligt til at rette fejl og mangler [19]. Ifølge Rigsrevisionen blev projektet afsluttet otte år forsinket med udgifter på 4,9 mia. kr. i 2025-priser, og nødvendige funktioner manglede fortsat [20].

I Australien måtte staten i 2020 nulstille eller tilbagebetale over 400.000 automatisk beregnede tilbagebetalingskrav; ifølge den efterfølgende undersøgelseskommission blev 746 mio. australske dollar tilbagebetalt til omkring 381.000 personer [21]. I Nederlandene indgik et selvlærende system i kontrollen med børnepasningsstøtte [22] som del af et bredere forløb, hvor titusinder af forældre har meldt sig som ramte, og hvor genopretningen i januar 2024 var budgetteret til over 7 mia. euro [23]. I Storbritannien var fejl i Horizon-regnskabssystemet knyttet til skønsmæssigt 983 domfældelser af postmestre [24], og staten afsatte i 2024 cirka 1,8 mia. pund til erstatninger [25].

Sagerne har forskellige årsager og vedrører ikke alle AI. De viser dog, hvor alvorlige følger fejl kan få, når kontrol og rettelse svigter. Datatilsynet advarede tilsvarende ved den første høring om store efterfølgende omkostninger, blandt andet ved forkerte afgørelser, hvis databeskyttelsesarbejdet forsømmes før ibrugtagning [2]. Krav til datakvalitet og rettelser bør derfor gælde al databehandling efter loven.

DSAM anbefaler:

- **at minimumskravene efter § 3, stk. 2, omfatter datakvalitet og håndtering af rettelser, afkræftelser og forbehold. Journalens rettelser skal slå igennem i AI-systemets datagrundlag og data til gentræning. Alvorlige fejl skal kunne markeres eller blokeres på tværs af systemer, så de ikke bruges som gældende oplysninger. Sundhedspersonen og patienten skal kunne kontrollere, hvilke oplysninger systemet har lagt til grund.**

- **at loven kræver datakvalitet og håndtering af rettelser ved al databehandling efter loven, også af andre oplysninger end helbredsoplysninger.**

2.2 Indsigt og patienttillid

Systemets indretning kan ikke i sig selv begrunde færre rettigheder

§ 4 giver ministeren mulighed for at begrænse rettigheder og forpligtelser efter GDPR artikel 12 og 15–21 inden for rammerne af GDPR artikel 23. Det omfatter blandt andet indsigt, rettelse, sletning og indsigelse. Bemærkningerne nævner teknisk kompleksitet (s. 77), men afviser generelle ressourcehensyn som eneste begrundelse (s. 78). Det svarer til Det Europæiske Databeskyttelsesråds retningslinjer, hvor udgifter og belastning af offentlige budgetter ikke i sig selv kan begrunde rettighedsbegrænsninger [26]. Oplysningspligten efter GDPR artikel 13 og 14 kan ikke begrænses efter § 4, og undtagelser følger af de øvrige databeskyttelsesregler (s. 43 og 79).

Efter DSAM's opfattelse gælder det samme for systemets tekniske indretning. Datatilsynet afviste i 2023, at Statens Serum Institut kunne undlade at opfylde oplysningspligten med henvisning til en uforholdsmæssigt stor indsats, blandt andet fordi systemet ikke var indrettet til at lette opgaven, eksempelvis gennem automatisering [27].

Før rettigheder begrænses efter § 4, bør det derfor dokumenteres, hvilke mindre indgribende løsninger der er undersøgt, herunder ændret systemindretning, og hvorfor de ikke er tilstrækkelige. Kan et system ikke understøtte den indsigt, rettelse og sletning, patienten har ret til, taler det helt imod brug til databehandling af følsomme helbredsoplysninger.

Rettighederne bør altså indbygges fra begyndelsen, som GDPR's krav om databeskyttelse gennem design forudsætter.

Retten til rettelse må ikke kunne begrænses

Ved AI kan samme fejl påvirke gentagne beslutninger om patienten, jf. afsnit 2.1. § 4 bør derfor ikke kunne begrænse retten til rettelse af helbredsoplysninger eller de tilknyttede garantier om begrænsning af databehandlingen og underretning af modtagere. De er nødvendige for, at rettelser og forbehold får virkning på tværs af systemer.

Beskyttelsen bør følge oplysningen

Helbredsoplysninger bør have samme beskyttelse i journaler, AI-træningsdata og kommunale eller nationale analysemiljøer. Det gælder tavshedspligt, indsigt, rettelse og de foreslåede fravalgsrettigheder, jf. afsnit 3.2. Selv om en begrænsning efter § 4 afgrænses til ét system, bør beskyttelsen række på tværs af systemerne.

Der skal være værn mod uvedkommende adgang, også gennem leverandører eller infrastruktur under andre landes lovgivning, og åbenhed om oplysningernes anvendelse. Det er afgørende for tilliden og patienternes villighed til at dele oplysninger til patientbehandling og forskning.

Rådet for Digital Sikkerhed rejste ved den første høring spørgsmålet, om personoplysninger opsamles hos udbydere af store AI-modeller, når myndigheder udvikler egne systemer, og anbefalede privatlivsfremmende teknologier i videst muligt omfang [28]. DSAM anbefaler, at konsekvensanalysen beskriver leverandørers og underleverandørers adgang til helbredsoplysninger, eventuelle overførsler til tredjelande og risikoen for brug til leverandørernes egne formål, herunder modeltræning, og at tekniske og aftalemæssige værn sikrer, at oplysningerne kun bruges til de fastlagte, lovlige formål.

DSAM anbefaler:

- **at § 4 ikke giver adgang til at begrænse retten til rettelse af urigtige helbredsoplysninger, retten til begrænsning af databehandlingen, mens rigtigheden undersøges, eller pligten til at underrette modtagere om rettelser og begrænsninger. Det samme gælder indsigelsesretten, jf. afsnit 3.2. Systemerne skal kunne håndtere rettelser og forbehold i datagrundlaget.**

2.3 Sammenstilling af oplysninger og adgang for andre myndigheder

Lovudkastet hjemler ikke videregivelse mellem myndigheder, men tillader genbrug af lovligt opbevarede oplysninger til AI-udvikling uden konkret forenelighedsvurdering. Profilering er udtrykkeligt omfattet af § 3, stk. 1, jf. afsnit 3.2.

Nye digitale infrastrukturer letter samtidig sammenstilling på tværs af områder. En kommune råder eksempelvis over oplysninger fra hjemmesygeplejen, beskæftigelsesområdet og socialområdet. Det giver ikke i sig selv adgang til at sammenstille dem. Lovbehandlingen bør afklare, hvilke sammenstillinger hjemlen tillader, og hvilke grænser der fortsat gælder.

Sammenstilling kan udlede følsomme forhold og sprede fejl mellem systemer, jf. afsnit 2.1. Store datasamlinger er også attraktive mål for cyberangreb. Europa-Kommissionens handlingsplan fra januar 2025 beskrev sundhedssektoren som EU's mest angrebne sektor gennem de foregående fire år og fremhævede forsinket diagnostik og patientbehandling som følge af angreb [29].

Socioøkonomiske oplysninger i AI til patientbehandling

Indenrigs- og Sundhedsministeriets projektbeskrivelse fra 2025 beskriver muligheder for at sammenstille sundhedsdata med personhenførbare og ikke-personhenførbare oplysninger om blandt andet uddannelse, indkomst og arbejdsmarkedstilknytning. Den nævner dataservices til AI og på længere sigt klinisk beslutningsstøtte [30]. Bekendtgørelsen om Ét Kontaktpunkt, delvist i kraft fra 1. august 2026, omfatter ansøgninger om videregivelse af sundhedsdata og andre relevante data til forskning og andre formål, og socioøkonomiske data nævnes udtrykkeligt [31].

Det giver ikke i sig selv hjemmel til klinisk beslutningsstøtte. Men med et relevant retsgrundlag kan modeller til patientbehandling komme til at bygge på oplysninger indsamlet til andre formål. Det kan gøre beslutningsgrundlaget mindre gennemskueligt for patienten og rettelser vanskeligere.

Socioøkonomiske oplysninger kan måske forbedre forudsigelser, men også skabe skævheder, afhængigt af modellens mål for behandlingsbehov. Et amerikansk system udpegede patienter til ekstra opfølgning ud fra forventede sundhedsudgifter. Det undervurderede systematisk sorte patienters behov, fordi der blev brugt færre penge på dem [32].

Flere oplysninger og mere komplekse modeller giver ikke automatisk bedre forudsigelser. En gennemgang fra 2019 fandt ingen sikker fordel ved maskinlæring frem for logistisk regression i kliniske prædiktionsmodeller [33], mens en metaanalyse fra 2023 om genindlæggelser fandt en lille fordel [34]. Værdien af socioøkonomiske oplysninger bør vurderes ved at sammenligne modellen med og uden oplysningerne i den tiltænkte patientgruppe. DSAM anbefaler, at merværdi og risiko dokumenteres før brug, og at patienten kan fravælge sammenstillingen.

AI-forordningens artikel 5, stk. 1, litra c, forbyder visse former for social bedømmelse ved hjælp af AI. Forbuddet omfatter AI-systemer, der over tid vurderer eller klassificerer personer eller grupper på grundlag af deres sociale adfærd eller kendte, udledte eller forudsagte personlige egenskaber eller personlighedstræk. Forbuddet gælder, når bedømmelsen fører til, at personer eller grupper stilles ringere, enten 1) i sociale sammenhænge uden forbindelse til dem, hvor oplysningerne oprindeligt blev genereret eller indsamlet, eller 2) på en måde, der er uberettiget eller uforholdsmæssig i forhold til deres sociale adfærd eller betydningen heraf [10].

Socioøkonomiske oplysninger i klinisk beslutningsstøtte er ikke i sig selv forbudt social bedømmelse. Hvis oplysninger fra skatte-, uddannelses- eller beskæftigelsesområdet skal påvirke patientbehandlingen, bør grænsen dog afklares. DSAM mener, at Folketinget udtrykkeligt bør fastlægge adgangen og betingelserne frem for at overlade dem til administrative beslutninger under en generel hjemmel. Dansk lov kan ikke tillade det, AI-forordningen forbyder.

Skævheder skal vurderes før brug

Risikoen for skævheder, herunder fra socioøkonomiske oplysninger, og følgerne for patienternes rettigheder skal undersøges og dokumenteres i konsekvensanalysen før brug, jf. afsnit 1.3. Dataetisk Råd anbefalede ved den første høring konkrete retningslinjer for kvalitetssikring med klare standarder for, hvilke niveauer af fejl, bias og uigennemsigtighed der er acceptable, før et system sættes i drift [3].

Adgang for politi og efterretningstjenester efter gældende ret

Politiets og efterretningstjenesternes adgang til datasamlinger følger af særskilte regler, ikke af AI-hjemlen. Efter § 4 i lov om Politiets Efterretningstjeneste (PET) skal andre forvaltningsmyndigheder efter anmodning videregive oplysninger til tjenesten uden forudgående retskendelse, hvis den vurderer, at oplysningerne må antages at have betydning for dens opgaver vedrørende straffelovens kapitel 12 og 13 [35]. Justitsministeren bekræftede i august 2025 over for DSAM, at det også gælder sundhedsoplysninger [36]. Efterretningstjenesterne er underlagt egne regler; GDPR's rettigheder til indsigt og rettelse følger ikke med oplysningerne, jf. databeskyttelseslovens § 3, stk. 2.

For oplysninger i den nationale genomdatabase findes et særskilt værn mod edition efter retsplejelovens § 804, dog med undtagelse for efterforskning af overtrædelser af straffelovens § 114 eller § 114 a (sundhedslovens § 223 b, stk. 2). Det illustrerer muligheden for særlig beskyttelse af datasamlinger, men vedrører en anden adgang til oplysninger end PET-lovens § 4. Datasamlinger til AI får ikke automatisk et tilsvarende værn.

Mulig ny PET-regulering og behovet for et værn

Et lovforslag fra april 2025 ville give PET adgang til »større sammenhængende datasæt« fra andre myndigheder ud fra datasættets samlede betydning for tjenestens opgaver, uden retskendelse eller individuel mistanke [37]. I et brev til DSAM af 27. august 2025 oplyste den daværende justitsminister, at helbredsoplysninger kunne indgå ved særligt vægtige hensyn, hele registre kun undtagelsesvis, og at genetiske oplysninger kunne kræve særskilt regulering [36]. Forslaget bortfaldt, men mulig ny regulering understreger behovet for at beskytte datasamlinger opbygget efter AI-hjemmelsloven.

DSAM foreslår derfor et lovfæstet værn for datasamlinger, der indeholder helbredsoplysninger og er opbygget efter loven: udlevering til politi og efterretningstjenester kun i konkrete sager, efter forudgående retskendelse og ved begrundet, individuel mistanke mod den person, oplysningerne vedrører. DSAM vil med værnet forebygge, at datasamlingerne gennem særskilte adgangsregler bliver tilgængelige for bred søgning og generel efterretningsmæssig analyse. Kravet om mistanke er bevidst; værnet ændrer ikke adgangen til at indhente oplysninger om eksempelvis ofre og vidner fra kildesystemerne, når betingelserne i de almindelige regler er opfyldt. Værnet bør omfatte hele datasamlingen og gælde på tværs af myndighedsområder, fordi helbredsoplysninger sammenstillet med andre oplysninger kan give et mere detaljeret billede af borgeren end kildesystemerne hver for sig. Det bygger på samme hensyn som genomdatabasens værn, men rækker bredere, og det bør gælde, før samlingerne etableres eller udbygges, uanset tidspunktet for ny PET-regulering. Tilsvarende værn bør overvejes for andre særligt følsomme oplysninger.

DSAM anbefaler:

- **at bekendtgørelser efter § 3, stk. 2, fastlægger tilladte oplysningskategorier i AI-systemer til patientbehandling. Oplysninger om økonomi, uddannelse og beskæftigelse fra andre forvaltningsområder skal kræve udtrykkelig lovhjemmel inden for AI-forordningens rammer. Merværdien skal dokumenteres for den konkrete anvendelse, og patienten skal kunne fravælge, at de indgår. Risikoen for skævheder skal undersøges i konsekvensanalysen, og patienten skal kunne se de anvendte oplysninger, jf. afsnit 1.2.**

- **at loven fastsætter et værn, så oplysninger fra datasamlinger, der indeholder helbredsoplysninger og er opbygget efter loven til AI-udvikling og -anvendelse, kun må udleveres til politi og efterretningstjenester i konkrete sager efter forudgående retskendelse og ved begrundet, individuel mistanke mod den person, oplysningerne vedrører. Der må ikke gives løbende søgeadgang eller adgang til hele datasamlinger til generel efterretningsmæssig analyse. Værnet skal omfatte hele datasamlingen og gælde på tværs af myndighedsområder. Forholdet til politiets og efterretningstjenesternes øvrige adgangs- og videregivelsesregler skal reguleres udtrykkeligt, og værnet skal indgå ved eventuel ny regulering af større sammenhængende datasæt.**

3. Klinisk anvendelse, genbrug og patientens selvbestemmelse

3.1 Automatiske afgørelser og reel menneskelig vurdering

Automatiske afgørelser skal udelukkes i selve lovteksten

DSAM finder det positivt, at bemærkningerne kræver reel, selvstændig menneskelig vurdering før afgørelser eller væsentlige tiltag over for den enkelte. Følger en sagsbehandler blot systemets forslag uden at tage stilling, er der ikke tale om reel beslutningsstøtte (s. 18). Det samme gælder en læge, der ukritisk følger et AI-forslag.

Afgrænsningen bør stå i lovteksten. § 2, nr. 4, definerer beslutningsstøtte som anvendelse, hvor systemet ikke selv træffer afgørelsen. Men § 3, stk. 1, hjemler AI »herunder« beslutningsstøtte og profilering og kan derfor læses som en bredere adgang.

GDPR artikel 22 beskytter mod afgørelser, der både er udelukkende automatiserede og har retsvirkning eller tilsvarende betydelig virkning for den enkelte. Sådanne afgørelser kan blandt andet tillades ved national lovgivning med passende garantier, jf. artikel 22, stk. 2, litra b. Datatilsynet påpegede uklarheden ved den første høring [2], og både Institut for Menneskerettigheder [6] og Dataetisk Råd [3] anbefalede en tydeligere afgrænsning af beslutningsstøtte i lovforslaget. DSAM anbefaler, at det i overensstemmelse med bemærkningerne udtrykkeligt fremgår af § 3, stk. 1, at loven ikke hjemler sådanne afgørelser.

Garantierne bør være bindende, særligt ved triagering og prioritering

Bemærkningerne fremhæver klar beslutningskompetence, dokumentation af afvigelser og logning som garantier for reel menneskelig vurdering, men gør dem ikke bindende (s. 19).

Det bør de være, især ved triagering, risikovurdering og henvisning. Lovforslaget nævner eksempelvis AI, der foreslår, hvilke patienter lægen skal tilse først (s. 64).

AI-forordningen kræver menneskeligt tilsyn med højrisikosystemer, herunder opmærksomhed på automatiseringsbias: tendensen til ukritisk at følge systemets anbefalinger [10]. Kravene omfatter ikke systemer uden for højrisikoklassifikationen, jf. afsnit 4.

Formel menneskelig medvirken er ikke en reel vurdering

Under tidspres og ved mange patienter kan AI-anbefalinger blive fulgt rutinemæssigt. Langvarig afhængighed af beslutningsstøtte kan desuden svække de kliniske færdigheder, som en kritisk vurdering kræver [14].

Kliniske beslutninger om prioritering, henvisning og patientbehandling kan have den betydelige virkning, GDPR artikel 22 omfatter. De europæiske databeskyttelsesmyndigheders retningslinjer nævner netop adgang til sundhedsydelser som eksempel [38].

En formel godkendelse er derfor ikke tilstrækkelig. Sundhedspersonen skal have faglig kompetence, kunne vurdere anbefalingens grundlag og have reel mulighed for at ændre beslutningen [38]. Dataetisk Råd foreslog ved den første høring, at beslutningsstøtte defineres ved, at en menneskelig beslutningstager har kompetence til, ansvar for og ressourcer til at træffe den endelige beslutning [3]. Datatilsynet fremhæver tilsvarende, at beslutningstageren skal kunne vurdere de faktiske oplysninger, og at grundlagets tilstrækkelighed og rigtighed skal kunne efterprøves [2], jf. afsnit 1.2 og 2.1.

I SCHUFA-dommen fastslog EU-Domstolen, at en automatisk beregnet kreditscore kan udgøre en afgørelse efter GDPR artikel 22, når den spiller en afgørende rolle for modtagerens beslutning om et aftaleforhold [39]. Efter DSAM's vurdering understøtter dommen, at en klinisk AI-anbefaling kan være omfattet, hvis den reelt bestemmer en beslutning med betydelig virkning for patienten uden selvstændig menneskelig vurdering. Også uden for GDPR artikel 22 skal kliniske beslutninger bygge på en selvstændig, fagligt forsvarlig vurdering.

Det bør efterprøves systematisk, om vurderingen fungerer i praksis. Det nederlandske datatilsyn anbefaler blandt andet at følge, hvor ofte brugerne fraviger forslagene, og teste med sager, hvor svaret er kendt [40]. Afvigelsesraten skal dog vurderes sammen med anbefalingerne og de konkrete beslutninger.

Journalen skal vise anbefalingen og den kliniske stillingtagen

Når AI-støtte har haft væsentlig betydning for undersøgelse, prioritering eller patientbehandling, bør journalen vise anbefalingen og sundhedspersonens stillingtagen, også når anbefalingen følges. Registreres kun afvigelser, mangler dokumentationen for, om fulgte anbefalinger blev selvstændigt vurderet.

Kravet bør indpasses i journalføringsreglerne. Tekniske detaljer kan opbevares særskilt, jf. afsnit 1.2. § 4 giver ikke hjemmel til at begrænse patientens ret til aktindsigt i journalen efter sundhedsloven.

Ansvarsfordelingen i almen praksis skal afklares
Private aktører kan ifølge bemærkningerne være omfattet, når databehandlingen sker som led i opgaver i samfundets interesse eller offentlig myndighedsudøvelse efter GDPR artikel 6, stk. 1, litra e (s. 58–60).

Almen praksis behandler typisk patientoplysninger efter GDPR artikel 6, stk. 1, litra c, og artikel 9, stk. 2, litra h. Om AI-baseret databehandling omfattes af den nye lov, afhænger dog af den konkrete opgave og betingelserne i artikel 6, stk. 1, litra e. Klinikkens sædvanlige retsgrundlag afgør derfor ikke spørgsmålet.

Lovbehandlingen bør afklare, om og i hvilket omfang almen praksis omfattes. I så fald skal minimumskravene efter § 3, stk. 2, også gælde her. Desuden skal rollerne som dataansvarlig og eventuel databehandler efter GDPR, fabrikant efter MDR samt udbyder og idriftsætter efter AI-forordningen afklares. Klinikken skal kende sit ansvar og sine dokumentationskrav, også ved systemer, som regionen har indkøbt eller stiller til rådighed. Falder anvendelsen uden for loven, bør det fremgå, hvilket retsgrundlag der i stedet gælder, herunder for regionale systemer.

DSAM anbefaler:

- **at bindende organisatoriske og faglige krav til reel menneskelig vurdering ved beslutningsstøtte med helbredsoplysninger fastsættes efter de relevante hjemler i databeskyttelses- og sundhedslovgivningen. Kravene skal omfatte klar beslutningskompetence, tilstrækkelig tid og de nødvendige faglige kompetencer til en selvstændig vurdering, mulighed for at fravige anbefalinger, dokumentation af klinisk stillingtagen, logning og løbende måling af afvigelser, jf. afsnit 1.2.**

- **at anbefalingen og sundhedspersonens kliniske stillingtagen journalføres, når AI-støtten har haft væsentlig betydning for undersøgelse, prioritering eller patientbehandling. Det skal også gælde fulgte anbefalinger og ske i overensstemmelse med journalføringsreglerne.**

- **at § 3, stk. 1, udtrykkeligt fastslår, at loven ikke hjemler automatiske individuelle afgørelser efter GDPR artikel 22.**

- **at lovens anvendelse i almen praksis afklares sammen med praksis', regioners og leverandørers roller og ansvar efter GDPR, MDR og AI-forordningen, herunder ved regionale systemer.**

3.2 Udvikling, gentræning og viderebehandling

Genbrug til udvikling og gentræning bør kræve en konkret vurdering
Lovforslaget tillader genbrug af lovligt opbevarede oplysninger, også fra afsluttede patientforløb, til AI-udvikling og gentræning uden konkret vurdering af, om formålet er foreneligt med det oprindelige. For helbredsoplysninger kræves fortsat en undtagelse efter GDPR artikel 9, stk. 2, og overholdelse af sundhedslovgivningens regler om anvendelse og tavshedspligt (s. 72).

Systemerne skal understøtte myndighedens eller organets opgaver efter anden lovgivning (§ 3, stk. 1, og s. 70–71).

En national hjemmel uden forenelighedsvurdering skal være nødvendig og forholdsmæssig for at varetage et hensyn i GDPR artikel 23, stk. 1, jf. artikel 6, stk. 4. Datatilsynet savnede ved den første høring en begrundelse for den brede adgang på tværs af myndigheder og sammenhænge og fremhævede den eksisterende mulighed for genbrug efter konkret forenelighedsvurdering [(2)]. Det reviderede udkasts generelle henvisning til GDPR artikel 23, stk. 1, eksempelvis litra e, giver efter DSAM's opfattelse fortsat ikke denne begrundelse (s. 25).

DSAM anbefaler en konkret forenelighedsvurdering ved genbrug af helbredsoplysninger til udvikling og gentræning. Fastholdes adgangen uden forenelighedsvurdering, skal lovhjemlens nødvendighed og forholdsmæssighed begrundes. Derudover bør hvert projekt afgrænses efter formål og datakategorier med dokumenteret nødvendighed, forholdsmæssighed og dataminimering. Patientbehandling, forskning og generel modeludvikling kan kræve forskellige retsgrundlag og garantier.

DSAM finder det positivt, at lovforslaget hverken hjemler videregivelse mellem myndigheder eller længere opbevaring af hensyn til AI-udvikling, end myndighedens øvrige opgaver tilsiger (s. 33–34 og 70–71).

Patienter bør kunne frabede sig brug til udvikling og gentræning

GDPR artikel 21 giver patienten ret til indsigelse mod databehandling som led i en offentlig opgave af grunde knyttet til patientens særlige situation. Retten er betinget, og den dataansvarlige kan fortsætte databehandlingen, hvis vægtige legitime grunde vejer tungere; den giver derfor ikke et frit fravalg. Den forudsætter desuden viden om anvendelsen, jf. afsnit 1.2.

DSAM foreslår derfor en enkel fravalgsret uden krav om begrundelse. Sundhedslovens § 29 giver en beslægtet mulighed, hvor patienten kan bestemme, at biologisk materiale afgivet ved patientbehandling kun må bruges til egen patientbehandling og umiddelbart tilknyttede formål, og kan træffe en tilsvarende beslutning om genetiske oplysninger udledt af materialet og opbevaret af Digital Sundhed Danmark (tidligere Nationalt Genom Center). Beslutningerne registreres i Vævsanvendelsesregisteret, som den ansvarlige myndighed eller sundhedsperson skal kontrollere før anden brug.

Fravalget bør omfatte al udvikling og gentræning med patientens helbredsoplysninger efter loven, også når formålet beskrives som patientbehandling, kvalitetsudvikling eller forskning. Rækkevidden skal fastlægges udtrykkeligt. Det vil efter DSAM's opfattelse styrke tilliden.

Patienter bør kunne fravælge klinisk AI i eget forløb

Brugen af AI, der er medicinsk udstyr, er efter DSAM's opfattelse en del af patientbehandlingen, jf. afsnit 4. Sundhedslovgivningens regler om information og selvbestemmelse gælder derfor også, når medicinsk AI indgår, og de kan ikke tilsidesættes med en hjemmel til databehandling. Reglerne giver dog ikke i sig selv ret til at fravælge klinisk AI og samtidig kræve, at sundhedspersonens vurdering foretages uden støtte i AI-forslag.

En sådan ret skal fastsættes udtrykkeligt.

DSAM foreslår derfor, at sundhedsloven giver patienten ret til at fravælge klinisk AI i egen udredning og patientbehandling, både AI-baseret beslutningsstøtte og anden AI-anvendelse med betydning for udredningen eller patientbehandlingen, så sundhedspersonens vurdering foretages uden støtte i AI-forslag. Retten gælder sundhedspersonens vurdering, ikke teknikken i sig selv; hvor AI er indbygget i apparatur eller systemer, indebærer fravalget, at vurderingen foretages uden at bygge på AI-forslaget. Loven bør fastlægge rækkevidden, information før brug og registrering af fravalget. Patienten skal kende AI's rolle og mulige betydning for beslutningerne, jf. afsnit 3.1. Fravalget skal kunne registreres i journalen og respekteres af regionens og praksis' systemer.

Muligheden skal indbygges fra starten, når AI bliver en integreret del af sundhedspersonens arbejdsredskaber, jf. afsnit 2.2. DSAM anbefalede også en udtrykkelig fravalgsret i høringssvaret om beslutningsstøtte [5].

Spørgsmålet blev rejst allerede i 2019 ved indførelsen af den bemyndigelse, der i dag står i sundhedslovens § 42 a, stk. 7, jf. afsnit 1.1. Et ændringsforslag om regler for fravalg af indhentning til beslutningsstøtte blev ikke vedtaget. Betænkningen viser dog, at både systematiske fejlbeslutninger og rettelse af urigtige oplysninger i den digitale infrastruktur blev drøftet [41]. Fravalgsretten i § 42 a, stk. 6, omfatter kun indhentning efter stk. 1 og 4. Folketinget bør tage spørgsmålet op igen, når grundlaget for AI-støttet patientbehandling udvides.

DSAM anbefaler:

- **at patienter får en enkel ret til at fravælge brug af deres helbredsoplysninger til udvikling og gentræning efter loven, uanset formålsbetegnelse, samt klinisk AI i egen udredning og patientbehandling, så sundhedspersonens vurdering foretages uden støtte i AI-forslag. § 4 må samtidig ikke kunne begrænse indsigelsesretten ved databehandling af helbredsoplysninger.**

- **at lovbehandlingen undersøger, om AI på andre områder kan have så indgribende konsekvenser, at borgeren altid bør kunne fravælge AI-baseret sagsbehandling.**

4. CE-mærkning af medicinsk AI og kontrol med egenudviklede systemer

CE-mærkning og ekstern vurdering understøtter patientsikkerheden

DSAM anbefaler som udgangspunkt CE-mærkning af AI, der er medicinsk udstyr. Mærkningen dokumenterer overensstemmelse med MDR's krav til blandt andet sikkerhed og ydeevne. Medicinsk software til beslutninger om diagnostik eller patientbehandling eller til overvågning af fysiologiske processer er som udgangspunkt klasse IIa eller højere efter MDR [42]. Her kræves vurdering ved et uafhængigt bemyndiget organ, og i disse risikoklasser er producentens egen vurdering ikke tilstrækkelig.

Undtagelsen placerer ansvaret for vurderingen hos institutionen

MDR artikel 5, stk. 5, tillader sundhedsinstitutioner at fremstille og bruge medicinsk udstyr uden CE-mærkning, når tilsvarende markedsførte produkter ikke tilstrækkeligt dækker patientmålgruppens særlige behov.
Institutionen skal dokumentere behovet, opfylde relevante sikkerheds- og ydeevnekrav, have et passende kvalitetsstyringssystem og offentliggøre en erklæring. Den skal følge erfaringerne fra klinisk brug og foretage nødvendige rettelser. Udstyret må ikke overføres til en anden retlig enhed (juridisk enhed) eller fremstilles i industriel målestok [43].

Undtagelsen omfatter også udstyr i klasse IIa, IIb og III. Institutionen kan dermed selv udvikle, vurdere og tage systemet i brug uden vurdering ved et bemyndiget organ. Myndighedernes tilsyn indebærer ikke en obligatorisk, uafhængig vurdering af hvert system før brug [43].

En regional fusion kan muliggøre omfattende intern anvendelse

Ifølge EU-vejledningen kan flere hospitaler udgøre én sundhedsinstitution, hvis de tilhører samme juridiske enhed og har fælles organisationsnummer, kvalitetsmål, kvalitetsstyringssystem og sundhedsstrategi, uanset geografisk placering [44]. Et fælles journalsystem er ikke et kriterium. Hverken MDR eller vejledningen fastsætter en antalsgrænse for hospitaler eller patienter.

Fremstillingen må dog ikke ske i industriel målestok. Begrebet er ikke nærmere defineret i MDR og vurderes konkret ud fra blandt andet omfang, kommercielle forhold og fremstillingsproces [44]. Afgrænsningen er vanskelig for software.

Region Hovedstaden og Region Sjælland bruger begge Sundhedsplatformen, men er to juridiske enheder. MDR's forbud mod overførsel mellem juridiske enheder kan derfor begrænse anvendelsen af egenudviklet udstyr på tværs af regionerne under undtagelsen [43].

Når de to regioner med tilsammen cirka 2,8 millioner borgere fusionerer til Region Østdanmark den 1. januar 2027, kan denne begrænsning bortfalde, hvis hospitalerne udgør én sundhedsinstitution inden for samme juridiske enhed, og alle øvrige betingelser er opfyldt. Sundhedsplatformen kan da lette udbredelsen af egenudviklet medicinsk AI uden CE-mærkning mellem hospitalerne. Selvstændige lægepraksisser bliver ikke del af enheden ved adgang til regionale systemer. Udstyret kan derfor ikke overføres til dem under undtagelsen.

DSAM finder det problematisk, at så omfattende klinisk anvendelse kan ske uden obligatorisk ekstern forhåndsvurdering. En organisatorisk fusion gør ikke i sig selv systemerne mere sikre.

Afgrænsningen er allerede aktuel. CLL-TIM, en maskinlæringsmodel, der forudsiger risikoen for alvorlig infektion eller behandlingsbehov hos nydiagnosticerede patienter med kronisk lymfatisk leukæmi, er ifølge udviklernes egen publikation fra 2024 implementeret under MDR artikel 5, stk. 5, som udstyr i klasse IIa med institutionens egen vurdering og uden CE-mærkning. Forfatterne begrunder dette med, at modellen kun var implementeret i ét journalsystem inden for en afgrænset organisation.

Publikationen beskriver også validering og vurdering i et klinisk råd, og forudsigelserne var mærket »research-use only«, fordi modellen fortsat blev afprøvet i et klinisk forsøg [45].

Ifølge udvikleren er modellen integreret i Sundhedsplatformen, som ejes og reguleres af Region Hovedstaden og Region Sjælland, og erfaringerne har allerede dannet baggrund for tilsvarende modeller inden for psykiatri og kardiologi [46]. Eksemplet understreger behovet for at afklare, hvordan betingelsen om samme juridiske enhed anvendes ved fælles journalsystemer.

AI-forordningen sikrer heller ikke generelt ekstern forhåndsvurdering

Ifølge den fælles, ikke-bindende EU-vejledning om MDR og AI-forordningen bliver medicinsk AI under MDR-undtagelsen ikke højrisikoklassificeret alene som følge af sin status som medicinsk udstyr, uanset risikoklasse, fordi undtagelsen ikke kræver vurdering ved et bemyndiget organ [47].

Højrisikokravene om blandt andet logning og menneskeligt tilsyn følger derfor ikke automatisk, selv ved betydelig klinisk risiko. Vejledningen varsler yderligere afklaring af reglerne for internt fremstillet medicinsk AI [47].

Akut patienttriage og visse andre anvendelser kan dog være højrisiko efter andre bestemmelser i AI-forordningen. For akut patienttriage kræver klassifikationen ikke i sig selv vurdering ved et bemyndiget organ [10]. Ønskes en uafhængig klinisk forhåndsvurdering, skal den derfor sikres særskilt.

Konsekvenserne for udbuddet af CE-mærket medicinsk AI bør belyses

Forskellige kontrolkrav kan påvirke udviklingen og udbuddet af medicinsk AI. Virksomheder, der markedsfører systemer i klasse IIa eller højere, betaler for CE-mærkning og vurdering ved et bemyndiget organ. Lovligt udviklede interne systemer er undtaget fra disse krav.

Den nye hjemmel til databehandling kan efter DSAM's vurdering gøre det lettere at udvikle og anvende egen medicinsk AI. DSAM er bekymret for, at undtagelsen dermed kan blive den mest anvendte vej, så flere systemer tages i brug uden uafhængig forhåndsvurdering. Det bør også afklares, hvordan kravet om manglende egnede alternativer håndhæves over tid. EU-vejledningen anbefaler, at institutionen løbende følger markedet og revurderer sin begrundelse. Bliver et mindst ligeværdigt CE-mærket produkt tilgængeligt, som tilstrækkeligt dækker patientgruppens særlige behov, bør institutionen begynde overgangen til det [44].

Følgevirkningerne bør belyses i denne lovbehandling

MDR tillader Danmark at begrænse fremstilling og brug af bestemte typer internt fremstillet udstyr. DSAM anbefaler at bruge muligheden, så kontrollen afspejler klinisk risiko og anvendelsens omfang [43].

§ 3, stk. 2, hjemler databeskyttelseskrav, men giver ikke et generelt grundlag for klinisk sikkerhedsregulering. Yderligere klinisk kontrol kræver derfor et andet eller udvidet lovgrundlag. Lægemiddelstyrelsen, Danske Regioner, kliniske fagmiljøer og branchen for medicinsk udstyr bør inddrages i vurderingen af patientsikkerhed, kontrol og produktudbud.

DSAM anbefaler i denne lovbehandling:

- **Bindende databeskyttelseskrav og særskilt regulering af klinisk ydeevne.** Minimumskravene efter § 3, stk. 2, skal også gælde databehandling efter loven i systemer under MDR-undtagelsen. Supplerende krav til dokumenteret klinisk ydeevne i den tiltænkte patientgruppe og arbejdsgang bør fastsættes inden for MDR og sundhedslovgivningen, om nødvendigt med en anden eller udvidet hjemmel. Kontrollen bør bygge på institutionernes eksisterende MDR-dokumentation, så dobbeltarbejde undgås.

- **Afklaring af ansvar og lovgrundlag før bred anvendelse.** Lovbehandlingen bør afklare behovet for supplerende klinisk kontrol, placeringen af ansvaret og behovet for opfølgende lovgivning. Det gælder også den løbende kontrol med MDR-undtagelsens betingelser og forståelsen af sundhedsinstitution og juridisk enhed ved dannelsen af Region Østdanmark den 1. januar 2027.

DSAM opfordrer samtidig til initiativer som led i eller i forlængelse af lovbehandlingen:

- **CE-mærkning ved betydelig klinisk risiko eller bred anvendelse.** Danmark bør inden for EU-rettens rammer begrænse MDR-undtagelsen for nærmere afgrænsede typer medicinsk AI i disse tilfælde, så de almindelige CE-krav skal opfyldes før brug.

- **Uafhængig vurdering af systemer, der fortsat bruges under undtagelsen.** En fagligt kvalificeret, uafhængig instans uden for den udviklende og anvendende organisation bør vurdere systemet før brug og ved væsentlige ændringer. Vurderingen skal tilpasses risiko og omfang, og instansen bør kunne stille bindende vilkår. Organisering og beføjelser kan fastlægges i opfølgende regulering.

5. Afsluttende bemærkninger

DSAM anerkender behovet for en generel AI-hjemmel i det offentlige og ser betydelige muligheder for bedre kvalitet og effektivitet. Anvendelsen kræver samtidig klare rammer og kontrol, især når AI påvirker beslutninger om den enkelte, og fejl kan gentages eller spredes til mange borgere.

Det gælder især for helbredsoplysninger og klinisk beslutningsstøtte. Sundhedsfaglige selskaber og patientrepræsentanter bør inddrages i de konkrete regler. Tillid til håndteringen af patientdata er afgørende for patientbehandling, forskning og kvalitetsudvikling og bør vægte centralt i lovbehandlingen.

Med venlig hilsen



Maria Krüger
Formand for DSAM

Referenceliste

1. Ingeniøren, AITech. Regeringen vil bane vejen for myndigheders brug af AI: »Der er nogle klare dataetiske betænkeligheder ved lovforslaget«. 18. september 2026. Tilgængelig på: https://pro.ing.dk/aitech/artikel/regeringen-vil-bane-vejen-myndigheders-brug-af-ai-der-er-nogle-klare-dataetiske-betaenkeligheder-ved
2. Datatilsynet. Høringssvar over udkast til forslag til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning. 3. marts 2026, j.nr. 2026-11-0479. Tilgængelig på: https://cdn.datatilsynet.dk/datatilsynet/Media/639251468025536342/hoeringssvar.pdf
3. Dataetisk Råd. Dataetisk Råds høringssvar til forslag til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning. 2. marts 2026. Tilgængelig på: https://www.dataetiskraad.dk/media/ty4orfig/dataetisk-ra-d-hoeringsvar-lov-om-udvikling-og-anvendelse-af-ai.pdf
4. Lov nr. 717 af 20. juni 2025 om ændring af sundhedsloven, lov om apoteksvirksomhed og lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter og sundhedsdatavidenskabelige forskningsprojekter, særligt sundhedslovens § 48 e. Tilgængelig på: https://www.retsinformation.dk/eli/lta/2025/717
5. Dansk Selskab for Almen Medicin. Høringssvar vedrørende udkast til bekendtgørelse om behandling af personoplysninger til brug for beslutningsstøtte ved patientbehandling. 14. januar 2026. Tilgængelig på: https://content.dsam.dk/guides/basissider/høringer/h2025-103-horingssvar.pdf
6. Institut for Menneskerettigheder. Høringssvar over lovforslag om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning. 7. april 2026, dok. nr. 26/00457-2. Tilgængelig på: https://menneskeret.dk/hoeringssvar/udvikling-anvendelse-ai-systemer-ved-behandling-personoplysninger-offentlige
7. Computerworld. Ekspert: Nyt lovforslag om brug af AI i offentlig sagsbehandling er farlig og »inviterer til ulovlig praksis«. 28. september 2026. Tilgængelig på: https://www.computerworld.dk/art/296962
8. Ingeniøren, AITech. Uafhængig it-rådgiver: Regeringen efterlader kommunerne med hele regningen i nyt AI-lovforslag. 2. oktober 2026. Tilgængelig på: https://pro.ing.dk/aitech/artikel/uafhaengig-it-raadgiver-regeringen-efterlader-kommunerne-med-hele-regningen-i-nyt-ai-lovforslag
9. Folketingets Ombudsmand. Ombudsmanden spørger til kommuners brug af AI til sagsbehandling. Nyhed af 18. august 2026. Tilgængelig på: https://www.ombudsmanden.dk/find-viden/nyheder/2026/ombudsmanden-spoerger-til-kommuners-brug-af-ai-til-sagsbehandling
10. Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens (AI-forordningen), som ændret ved forordning (EU) 2026/1744 af 8. juli 2026, særligt artikel 5, stk. 1, litra c, om social bedømmelse, artikel 10 om data og datastyring, artikel 12 om automatisk registrering af hændelser i højrisiko-AI-systemer, artikel 14, stk. 4, litra b, om menneskeligt tilsyn, artikel 26, stk. 4, om idriftsætterens kontrol med inputdata, artikel 26, stk. 6, om idriftsætterens opbevaring af logfiler samt bilag III, punkt 5, litra a og d. Tilgængelig på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32024R1689 (konsolideret udgave: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:02024R1689-20260727)
11. Europa-Parlamentets og Rådets forordning (EU) 2026/1744 af 8. juli 2026 om ændring af forordning (EU) 2024/1689, (EU) 2018/1139 og (EU) 2023/1230 for så vidt angår forenkling af gennemførelsen af harmoniserede regler om kunstig intelligens (digital omnibus om kunstig intelligens). Tilgængelig på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32026R1744
12. Bekendtgørelse nr. 1361 af 24. november 2025 om autoriserede sundhedspersoners patientjournaler (journalføring, opbevaring, videregivelse, overdragelse m.v.), §§ 11, 20 og 35. Tilgængelig på: https://www.retsinformation.dk/eli/lta/2025/1361
13. Artikel 29-Gruppen. Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen »sandsynligvis indebærer en høj risiko« i henhold til forordning (EU) 2016/679. WP 248 rev. 01, senest revideret og vedtaget den 4. oktober 2017; videreført af Det Europæiske Databeskyttelsesråd. Særligt s. 15–17 og 21. Tilgængelig på: https://cdn.datatilsynet.dk/datatilsynet/media/7826/konsekvensanalyser-vedroerende-databeskyttelse-dpia-wp248.pdf

14. Kristiansen TB, Kristensen K, Uffelmann J, Brandslund I. Erroneous data: The Achilles' heel of AI and personalized medicine. Frontiers in Digital Health. 2022;4:862095. Tilgængelig på: https://doi.org/10.3389/fdgth.2022.862095

15. Nielsen AA, Christensen H, Lund ED, Christensen C, Brandslund I, Green A. Diabetes mortality differs between registers due to various disease definitions. Danish Medical Journal. 2014;61(5):A4840. Tilgængelig på: https://ugeskriftet.dk/dmj/diabetes-mortality-differs-between-registers-due-various-disease-definitions

16. Greibe T. Fejlkodning af diabetes II og datafangst – eller de 10 små cyklister med sukkersyge, der endte med at være 8½. Månedsskrift for Almen Praksis. 2014;(8). Tilgængelig på: https://www.maanedsskrift.dk/arkiv/2014/207/10985/

17. Sator L, Horner A, Studnicka M, Lamprecht B, Kaiser B, McBurnie MA, et al. Overdiagnosis of COPD in subjects with unobstructed spirometry: a BOLD analysis. Chest. 2019;156(2):277–288. Tilgængelig på: https://doi.org/10.1016/j.chest.2019.01.015

18. Ellesøe SG, Jensen AB, Ängquist LH, Hjortdal VE, Larsen LA, Brunak S. How suitable are registry data for recurrence risk calculations? Validation of diagnoses on 1,593 families with congenital heart disease. World Journal for Pediatric and Congenital Heart Surgery. 2016;7(2):169–177. Tilgængelig på: https://doi.org/10.1177/2150135115615786

19. Vurderingsstyrelsen. Er der fejl eller mangler i dine BBR-oplysninger? Tilgængelig på: https://www.vurderingsportalen.dk/ejerbolig/vurdering/bbr/

20. Rigsrevisionen. Rigsrevisionens notat om beretning om Skatteministeriets styring af det nye ejendomsvurderingssystem. RN 1509/25, 21. november 2025 (udgivet december 2025). Tilgængelig på: https://www.rigsrevisionen.dk/Media/638998268925610237/1509-25.pdf

21. Royal Commission into the Robodebt Scheme. Report, Volume 1, s. xi og xxviii–xxix. 7. juli 2023 (rettet udgave 11. juli 2023). Tilgængelig på: https://robodebt.royalcommission.gov.au/

22. Tweede Kamer der Staten-Generaal. Parlementaire enquête fraudebeleid en dienstverlening. Lijst van vragen en antwoorden. Kamerstuk 35 867, nr. 8. 5. april 2024, svar på spørgsmål 33. Tilgængelig på: https://zoek.officielebekendmakingen.nl/kst-35867-8.html

23. NOS. De Toeslagenaffaire: van een miljoenen- naar een miljardenoperatie. 6. januar 2024. Tilgængelig på: https://nos.nl/artikel/2503966-de-toeslagenaffaire-van-een-miljoenen-naar-een-miljardenoperatie

24. House of Lords Library. Post Office Horizon IT scandal: Progress of compensation. 20. februar 2025. Tilgængelig på: https://lordslibrary.parliament.uk/post-office-horizon-it-scandal-progress-of-compensation/

25. House of Commons Library. Autumn Budget 2024: A summary. Research briefing CBP-10124, 31. oktober 2024. Tilgængelig på: https://commonslibrary.parliament.uk/research-briefings/cbp-10124/

26. Det Europæiske Databeskyttelsesråd. Retningslinjer 10/2020 om begrænsninger i henhold til artikel 23 i databeskyttelsesforordningen. Version 2.0, 13. oktober 2021, afsnit 3.3.3. Tilgængelig på: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en

27. Datatilsynet, afgørelse af 2. februar 2023 vedrørende Statens Serum Instituts opfyldelse af oplysningspligten, j.nr. 2021-432-0070. Tilgængelig på: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/statens-serum-instituts-opfyldelse-af-oplysningspligten

28. Rådet for Digital Sikkerhed. Høringssvar til Digitaliseringsministeriets udkast til forslag til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning. 28. februar 2026. Tilgængelig på: https://www.digitalsikkerhed.dk/wp-content/uploads/2026/02/RfDS-hoeringssvar-lovudkast-AI-i-det-offentlige-28.2.26.pdf

29. Europa-Kommissionen. European action plan on the cybersecurity of hospitals and healthcare providers. COM(2025) 10 final, 15. januar 2025. Tilgængelig på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:52025DC0010

30. Indenrigs- og Sundhedsministeriet. En ny, national indgang til sundhedsdata til forskning og innovation. Beskrivelse af projekt til realisering af trin 1 af visionen for bedre brug af sundhedsdata. Udateret, offentliggjort januar 2025. Tilgængelig på:

https://sundhedsdatastyrelsen.dk/Media/638731414365577770/Projektbeskrivelse-realisering-af-visionen-for-bedre-brug-af-sundhedsdata-trin1.pdf

31. Bekendtgørelse nr. 627 af 30. juni 2026 om Ét Kontaktpunkt, § 1 og § 5, nr. 5. Tilgængelig på: https://www.retsinformation.dk/eli/lta/2026/627
32. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366(6464):447–453. Tilgængelig på: https://doi.org/10.1126/science.aax2342
33. Christodoulou E, Ma J, Collins GS, Steyerberg EW, Verbakel JY, Van Calster B. A systematic review shows no performance benefit of machine learning over logistic regression for clinical prediction models. Journal of Clinical Epidemiology. 2019;110:12–22. Tilgængelig på: https://doi.org/10.1016/j.jclinepi.2019.02.004
34. Talwar A, Lopez-Olivo MA, Huang Y, Ying L, Aparasu RR. Performance of advanced machine learning algorithms over logistic regression in predicting hospital readmissions: A meta-analysis. Exploratory Research in Clinical and Social Pharmacy. 2023;11:100317. Tilgængelig på: https://doi.org/10.1016/j.rcsop.2023.100317
35. Lov om Politiets Efterretningstjeneste (PET), jf. lovbekendtgørelse nr. 231 af 7. marts 2017 med senere ændringer, § 4 (stk. 2 og 3 ophævet ved lov nr. 1706 af 27. december 2018). Tilgængelig på: https://www.retsinformation.dk/eli/lta/2017/231
36. Justitsministeren (Peter Hummelgaard). Brev af 27. august 2025 til Dansk Selskab for Almen Medicin som svar på selskabets henvendelse af 1. juli 2025, offentliggjort som endeligt svar på spørgsmål nr. 55 til L 218 (folketingsåret 2024-25). Tilgængelig på: https://www.ft.dk/samling/20241/lovforslag/L218/spm/55/svar/2157358/3059009.pdf
37. Forslag til lov om ændring af lov om Politiets Efterretningstjeneste (PET) (Understøttelse af Politiets Efterretningstjenestes mulighed for at udføre data- og analysebaseret efterretningsvirksomhed m.v.). L 218, folketingsåret 2024-25, fremsat af justitsministeren den 25. april 2025, forslag til § 10 c; bortfaldet uden vedtagelse. Tilgængelig på: https://www.retsinformation.dk/eli/ft/202412L00218
38. Artikel 29-Gruppen. Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning (EU) 2016/679. WP 251 rev. 01, senest revideret og vedtaget den 6. februar 2018; videreført af Det Europæiske Databeskyttelsesråd. Tilgængelig på: https://ec.europa.eu/newsroom/article29/items/612053
39. EU-Domstolen. Dom af 7. december 2023 i sag C-634/21, SCHUFA Holding (Scoring). Tilgængelig på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:62021CJ0634
40. Autoriteit Persoonsgegevens. Meaningful Human Intervention: A tool for shaping and implementing meaningful human intervention. Juli 2025. Tilgængelig på: https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2025-07%2FMeaningful+Human+Intervention.pdf
41. Sundheds- og Ældreudvalget. Betænkning over Forslag til lov om ændring af sundhedsloven (Bedre digitalt samarbejde i sundhedsvæsenet, påmindelser til forældre vedrørende børnevaccination og bestemmelser om territorial gyldighed for Færøerne og Grønland), L 127, folketingsåret 2018-19. Afgivet den 26. februar 2019, ændringsforslag nr. 5 og 9 med bemærkninger samt de politiske bemærkninger. Tilgængelig på: https://www.ft.dk/ripdf/samling/20181/lovforslag/l127/20181_l127_betaenkning.pdf (også på https://www.retsinformation.dk/eli/ft/201814L00789)
42. MDCG 2019-11 rev. 1, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, juni 2025. Tilgængelig på: https://health.ec.europa.eu/document/download/b45335c5-1679-4c71-a91c-fc7a4d37f12b_en?filename=md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf
43. Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr (MDR), særligt artikel 5, stk. 5, artikel 52 og bilag VIII, regel 11. Tilgængelig på: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:32017R0745
44. MDCG 2023-1, Guidance on the health institution exemption under Article 5(5) of Regulation (EU) 2017/745 and Regulation (EU) 2017/746, januar 2023. Tilgængelig på: https://health.ec.europa.eu/system/files/2023-01/mdcg_2023-1_en.pdf

45. Agius R, Riis-Jensen AC, Wimmer B, da Cunha-Bang C, Murray DD, Poulsen CB, Bertelsen MB, Schwartz B, Lundgren JD, Langberg H, Niemann CU. Deployment and validation of the CLL treatment infection model adjoined to an EHR system. npj Digital Medicine. 2024;7:147. Tilgængelig på: https://doi.org/10.1038/s41746-024-01132-6

46. Niemann CU. Datadrevet lægekunst ligger implicit i lægeløftet. Kronik, Dansk Selskab for ledelse i Sundhedsvæsenet, 23. september 2026. Tilgængelig på: https://dssnet.dk/datadrevet-laegekunst-ligger-implicit-i-laegeloeftet/

47. AIB 2025-1 / MDCG 2025-6, Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA), juni 2025, spørgsmål 35. Tilgængelig på: https://health.ec.europa.eu/document/download/b78a17d7-e3cd-4943-851d-e02a2f22bbb4

Notat
Dato 9. oktober 2026
MAVI/EHP

Dansk Socialrådgiverforening
faglig handlekraft

Til Digitaliseringsstyrelsen

Høringssvar fra Dansk Socialrådgiverforening til Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Dansk Socialrådgiverforening har valgt at afgive høringssvar til dette lovudkast, fordi loven vil få betydning for socialrådgivere, der i vid udstrækning arbejder med sårbare borgere på offentlige myndighedsområder.

DS anerkender behovet for et klarere retsgrundlag for anvendelsen af AI i den offentlige sektor og dermed nødvendigheden af lovforslaget. AI-løsninger kan efter DS' opfattelse understøtte og kvalificere den offentlige opgaveløsning. Samtidig er det afgørende at understrege, at anvendelsen af AI på det sociale område rejser grundlæggende spørgsmål om retssikkerhed, faglighed og borgernes tillid til den offentlige forvaltning. Ambitionerne om effektivisering og øget kvalitet må ikke føre til, at der gås på kompromis med disse hensyn.

Generelle bemærkninger

For det første er det afgørende for Dansk Socialrådgiverforening (DS), at anvendelsen af kunstig intelligens ikke fører til personalereduktioner. Ressourcer, der eventuelt frigøres ved brug af AI, bør i stedet anvendes til at styrke kvaliteten i opgaveløsningen. Det gælder navnlig den relationelle kontakt med børn og voksne samt muligheden for at foretage en helhedsorienteret vurdering af den enkelte borgers situation. Begge dele er afgørende for borgerens retssikkerhed og for den faglige kvalitet.

DS ønsker at understrege, at anvendelsen af AI ikke stiller færre, men flere krav til socialrådgiverens faglighed. Når kunstig intelligens indgår i sagsbehandlingen, øges behovet for professionel dømmekraft, herunder evnen til at forstå og kritisk vurdere de output, som AI-systemet leverer. Det forudsætter et højt socialfagligt niveau og relevante AI-kompetencer samt en systematisk og vedvarende opkvalificering af medarbejderne. DS finder det afgørende, at arbejdsgiveren påtager sig et klart ansvar for de ansattes anvendelse af AI-systemer og sikrer løbende kompetenceudvikling gennem uddannelse, den fornødne tid og organisatorisk understøttelse.

Det fremgår af lovbemærkningerne, at indførelsen af AI-systemer hos offentlige myndigheder skal medføre effektiviseringsgevinster og frigive tid til kerneopgaven. Der peges på, at lovforslaget især kan medføre økonomiske omkostninger i forbindelse med implementeringen af AI-systemerne, men det forventes, at disse omkostninger efterfølgende opvejes af gevinsterne ved at anvende systemerne. DS er skeptisk over for denne vurdering. Udvikling og implementering af AI-systemer må forventes at foregå løbende, og der vil desuden være vedvarende omkostninger til kontrol af, at reglerne overholdes, og til tilsyn med, at systemerne fungerer efter hensigten. Hertil kommer, at energiforbruget og betalingen for anvendelsen af systemerne formentlig vil stige i fremtiden.

DS ønsker desuden at kvittere for, at der med det nye lovforslag ikke etableres en generel hjemmel til at videregive og samkøre data på tværs af myndigheder. Der er tale om en vigtig præcisering, der beskytter borgeren.

Endelig vil DS pege på behovet for AI-personalepolitikker på de offentlige arbejdspladser. Personalepolitikken bør sikre medarbejderinddragelse ved indkøb, udvikling, implementering og evaluering af AI-systemer. De bør desuden indeholde tiltag, der forebygger, at faglige kompetencer eroderes, arbejdet intensiveres, frygten for at miste jobbet stiger, overvågning af medarbejderne øges, og – at meningen med arbejdet og arbejdstilfredsheden falder.

Specifikke bemærkninger

Beslutningsstøtte

DS finder det positivt, at lovforslaget indeholder begrebsdefinitioner, som kan støtte myndighederne og deres ansatte i udviklingen, implementeringen og anvendelsen af AI-systemer. Det er ligeledes positivt, at lovforslaget definerer 'beslutningsstøtte' og præciserer, at AI-systemer aldrig må træffe automatiserede afgørelser, men at der skal være en fysisk person, som inddrager AI-systemets forslag i den samlede konkrete individuelle faglige vurdering, som ligger til grund for den endelige afgørelse.

DS er dog bekymret for, om socialrådgiveren i praksis får de nødvendige forudsætninger for selvstændigt at kunne bedømme og vurdere AI-systemets forslag til afgørelse. Denne bekymring bygger på flere forhold.

- DS ser en risiko for, at AI-systemer udformes, så socialrådgiverens bedømmelse og endelige afgørelse i praksis reduceres til at sætte flueben ved 'Sagen er vurderet' og 'AI-systemets anbefaling godkendes'. Et sådant systemdesign vil gøre den menneskelige vurdering til en formalitet. Det vil være ulovligt og dermed udgøre et potentielt retssikkerhedsproblem.

- Socialrådgivere har som oftest meget travlt, og altid i gang med flere - somme tider akutte - borgersager samtidig. Der kan derfor være risiko for, at socialrådgiverne i praksis ikke har den nødvendige tid til rådighed til at kunne lave en grundig vurdering af alle sager.
- Nyuddannede og nyansatte socialrådgivere vil være mere afhængige af hjælpen fra et AI-system og have sværere ved at gennemskue og udfordre AI-systemets anbefalinger. Der kan derfor være risiko for, at de hurtigere accepterer anbefalingerne fra AI-systemet og på længere sigt vænner sig til, at dette bliver normen.

I bemærkningerne til lovforslaget anerkendes det, at scenariet, hvor AI-systemet gør det nemt at acceptere beslutningsstøtten som den endelige afgørelse, kan udgøre en reel risiko. Det fremgår også, at et sådant system vil være ulovligt. Lovbemærkningerne angiver imidlertid ikke, hvor omfattende den menneskelige involvering skal være, før der er tale om beslutningsstøtte frem for en fuldautomatisk afgørelse. Her henvises blot til, at fremtidig praksis vil bidrage til en præcisering.

Der skitseres nogle initiativer, arbejdspladsen kan anvende, f.eks. at identificere, hvem der har beslutningskompetencen, og sikre dokumentation og logning af processerne. Der gives imidlertid ikke klare anvisninger på, hvordan man undgår eller forebygger, at beslutningsstøtten i praksis ændrer karakter til en beslutning, eller hvordan det sikres, at socialrådgiveren får reel mulighed for at foretage en vurdering, herunder opdage fejlbehæftede eller skæve AI-anbefalinger. Det fremgår heller ikke, hvordan dette kontrolleres.

Profilering

Lovforslaget giver konkret mulighed for fremover at profilere borgere, dvs. evaluere bestemte forhold hos borgere på baggrund af personoplysninger. Ifølge lovforslagets bemærkninger forventes det, at AI-systemerne kan trænes på historiske og afsluttede sager for at kunne levere redskaber til at profilere (evaluere) den konkrete borger og dennes udfordringer, og dermed at kunne levere beslutningsstøtten, dvs. forslag til afgørelser. Her ser DS en risiko for, at AI-systemerne vil kunne levere beslutningsstøtte, som ikke matcher borgerens reelle behov. Det er der flere grunde til:

- AI-systemets profilering af borgeren og dennes sag risikerer alene at tage udgangspunkt i statistiske sandsynligheder. Dermed kan AI-systemet overse de unikke forhold i borgerens sag, som taler for en anden afgørelse end den, beslutningsstøtten lægger op til. Sociale sager er ofte komplekse og forskelligartede, og det kræver både dyb og bred faglighed at nå frem til den rette afgørelse. Derfor er en konkret og individuel vurdering nødvendig, men som beskrevet ovenfor er der risiko for, at denne vurdering i praksis udelades.
- Når AI-systemet skal trænes på gamle sager, vil der være en stor risiko for, at sagerne reelt er forældede fordi lovgrundlaget eller lovfortolkningen har

ændret sig, eller fordi AI-systemets anbefaling ikke tager afsæt i de nyeste sociale metoder og redskaber.
- Endelig kan der være bias i gamle sager i form af forforståelse af særlige samfundsgrupper eller problematikker, som har ændret sig.

I bemærkningerne til lovforslaget gøres opmærksom på risici ved profilering og bias, men der begrænset vejledning om, hvordan disse risici kan håndteres. Det overlades til myndigheden selv at vurdere, hvilke mitigerende foranstaltninger, der kan være relevante.

Ressortministeriernes opgave
Det fremgår af bemærkningerne til lovforslaget, at myndigheder, der arbejder med sårbare borgere, i realiteten bør udarbejde passende og specifikke foranstaltninger til beskyttelse af borgeres rettigheder og interesser. På den baggrund finder DS det besynderligt, at lovforslaget ikke forpligter ressortministerierne – men kun opfordrer - til at gennemføre en vurdering af behovet for yderligere foranstaltninger til beskyttelse af borgere inden for deres ressortområde.

På det sociale område arbejdes der netop med følsomme personoplysninger om borgernes helbred, sociale problemer, misbrug, handicap, sygdomme, kriminalitet samt ikke mindst om børns forhold.

DS mener, at det er nødvendigt, at ressortministerierne løbende gennemfører sådanne vurderinger, så borgerne kan beskyttes bedst muligt, idet udviklingen af AI sker med stor hast.

Da AI-forordningen har udsat igangsættelsen af AI-systemer på følsomme områder til udgangen af 2027, bør ressortministerierne, herunder Socialministeriet, have tid til at gennemføre denne opgave.

Undtagelser til den registreredes rettigheder
Lovforslaget giver ressortministerierne mulighed for at indføre begrænsninger af de rettigheder, som borgeren har efter databeskyttelsesforordningen, herunder retten til indsigt og sletning. Som begrundelse henvises der til, at det i praksis kan være vanskeligt at udskille en borgers data fra et komplekst AI-system. DS er bekymret for, om denne adgang kan føre til generelle og vidtgående begrænsninger for et helt ressortområde, eller om begrænsningerne alene vil kunne knyttes til bestemte systemtyper eller opgaver. Lovforslagets mulige rækkevidde fremstår derfor uklar.

I den forbindelse vil DS gøre opmærksom på, at borgernes tillid til myndighederne i høj grad er betinget af gennemsigtige og gennemskuelige processer, og at en svækkelse af borgerens ret til indsigt kan øge mistilliden – ikke alene til socialrådgiveren – men til de offentlige myndigheder som sådan.

I forhold til anvendelse af AI-systemerne i den konkrete sagsbehandling vil en borger med rette kunne spørge til, om AI har været brugt til behandlingen af borgerens sag, hvordan og i hvilket omfang. DS ønsker at gøre opmærksom på, at jo tættere AI-teknologien kommer på afgørelser om udsatte borgeres liv, desto stærkere skal kravene være til retssikkerheden. Det skal kunne forklares, hvordan en afgørelse er blevet til.

Ansvarsproblematik
DS ønsker at gøre opmærksom på en særlig usikkerhed ved brugen af eksterne offentligt tilgængelige AI-systemer. Det fremgår indirekte af bemærkningerne i lovforslaget, at AI-systemerne ejes af den offentlige myndighed, som dermed også er ansvarlig både for datasikkerhed i AI-systemerne og for de ansattes anvendelse af AI-systemerne. Det er imidlertid uklart, hvordan de ansatte er stillet ved brug af andre offentligt tilgængelige AI-systemer, chatbots og apps, f.eks. ChatGPT, Google Gemini, Claude, Le Chat og Grok. Det er heller ikke umiddelbart gennemskueligt i lovbemærkningerne, om de ansatte må anvende disse systemer som supplement til de AI-systemer, som arbejdspladsen stiller til rådighed.

DS anbefaler, at arbejdsgiveren vejleder de ansatte om, at anvendelse af andre offentlig tilgængelige AI-systemer bør undgås, herunder klargør, hvad der er tilladt og hvad der ikke er tilladt at bruge. Formålet er at forebygge, at ansatte utilsigtet uploader personoplysninger eller anvender utilstrækkeligt fagligt underbyggede forslag som grundlag for afgørelser og dermed påtager sig et individuelt ansvar i sagsbehandlingen, der ikke er omfattet af de systemer, som arbejdsgiveren har indført og har ansvar for.

Derudover bør den offentlige myndighed tage tydeligt stilling til, hvem der har det organisatoriske ansvar for valg af AI-system, udvikling, kvalitetssikring, kontrol, instruktion, dokumentation, kompetenceudvikling samt håndtering af fejl. Det skal herunder afklares, hvordan ansvaret fordeles mellem myndigheden, leverandøren, ledelsen, så man undgår at ansvaret havner på hos den enkelte bruger af AI-systemet.

Endelig vil DS fremhæve, at forskelle i kommunernes indførelse, implementering og anvendelse af AI-systemer kan føre til, at borgerne ikke mødes af samme niveau af databeskyttelse, service og hjælp. Der er derfor behov for tværgående minimumsstandarder, som kan understøtte en mere ensartet og retssikker anvendelse af AI-systemer på tværs af kommuner og andre offentlige myndigheder.

Opsummering

- AI-systemer må gerne understøtte og styrke – men ikke erstatte det socialfaglige skøn.

- Det skal være reelt muligt for socialrådgiveren at vurdere AI-genererede forslag. Det forudsætter tilstrækkelig tid, kompetencer og adgang til de oplysninger, som forslaget bygges på samt mulighed for at fravige anbefalingen og få organisatorisk opbakning til at gøre det.
- Borgeren skal kunne få klarhed over, om og hvordan AI har indgået i sagsbehandlingen, herunder med hvilket formål og med hvilken betydning for sagen. Det skal desuden fremgå, hvordan den efterfølgende faglige vurdering er foretaget.
- Det sociale område er særligt risikofyldt i forhold til anvendelse af AI, idet der i stor udstrækning behandles følsomme personoplysninger i komplekse sager med sårbare borgere. Derfor skal beskyttelsen og gennemsigtigheden være høj.
- Der skal være et tydeligt ansvar for kvalitetssikring og kontrol af AI-systemer, så den enkelte medarbejder ikke pålægges ansvaret for systemfejl. Der skal ligeledes være tydelige grænser for hvilke AI-systemer den ansatte må bruge til løsning af arbejdsopgaverne.
- AI skal frigive tid til at styrke den faglige kvalitet og kontakten med borgeren. Eventuelle effektiviseringsgevinster må ikke anvendes til at intensivere arbejdet, så socialrådgiveren skal håndtere og være i kontakt med endnu flere borgere end i dag.

Med venlig hilsen

Marie Vithen

Næstforkvinde
Dansk Socialrådgiverforening

Digitaliseringsstyrelsen
Landgreven 4
Sendt til: jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk, og kahevi@digst.dk

9. oktober 2026

Høringssvar over AI-hjemmelsloven

Danske Advokater takker for muligheden for at afgive høringssvar. Dette høringssvar er udarbejdet i samarbejde med Danske Advokaters fagudvalg for databeskyttelse og fagudvalg for teknologi.

Danske Advokater støtter forslaget til AI-hjemmelsloven og er positive over for udvidelsen af anvendelsesområdet og de øvrige justeringer, der er foretaget i lovforslaget siden høringen i februar 2026.

I det reviderede lovforslag er blandt andet tilføjet bemærkninger om viderebehandling af oplysninger. Der står nu, at:

> ”Den foreslåede ordning vil medføre, at der vil blive etableret et grundlag for viderebehandling af personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 4, som myndigheden allerede er i besiddelse af og har lovlig adkomst til, hvilket dermed omfatter personoplysninger fra historiske og lukkede sager. Det skyldes, at den foreslåede ordning klart og tydeligt vil angive, at der vil kunne ske udvikling af AI-systemer på baggrund af personoplysninger, som myndigheden (i forvejen) behandler.” Citat side 34 i lovforslaget.

Danske Advokater finder, at ordlyden ”efter anden lovgivning” i lovforslagets § 3, stk. 1, kan give anledning til fortolkningstvivl om adgangen til en sådan viderebehandling.

Danske Advokater anbefaler derfor, at det præciseres direkte i § 3, stk. 1, at bestemmelsen også etablerer et grundlag for viderebehandling af personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 4, som myndigheden allerede er i besiddelse af og har lovlig adkomst til, som beskrevet i bemærkningerne.

Afsluttende bemærkninger

Danske Advokater står gerne til rådighed for uddybende spørgsmål eller dialog.

Med venlig hilsen

Charlotte Hvid Olavsgaard
Juridisk konsulent
Danske Advokater

Høringssvar

DANSKE PROFESSIONSHØJSKOLER

Oktober 2026
Ref.: MBD
J.NR.: 2015-0073/262470

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Att. Jonathan Meijer

Danske Professionshøjskoler
Vester Voldgade 107
1552 København K
Tel. 9292 3575
info@dkprof.dk

Høringssvar: Høring over udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Danske Professionshøjskoler takker for indkaldelsen til høring over udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Vi har følgende bemærkninger:

Generelle bemærkninger:

Danske Professionshøjskoler er positive over for lovforslagets formål om at etablere et tydeligere og mere generelt databeskyttelsesretligt grundlag for offentlige myndigheders og organers mulighed for at udvikle og anvende AI-systemer ved behandling af personoplysninger.

Danske Professionshøjskoler vurderer, at lovforslaget kan bidrage til større sikkerhed om retsstillingen på området, såfremt anvendelsen af kunstig intelligens sker ansvarligt og med den nødvendige beskyttelse af de registreredes rettigheder og retssikkerhed.

Specifikke bemærkninger:

Eksempler fra uddannelses- og forskningsområdet

Danske Professionshøjskoler anbefaler, at der i lovbemærkningerne til § 1 og § 3, stk. 1 samt i det varslede vejledningsmateriale indgår eksempler fra uddannelses- og forskningsområdet. Dette vil tydeliggøre, i hvilket omfang loven kan udgøre et supplerende retsgrundlag for anvendelse af AI i professionshøjskolernes lovbestemte opgaver, hvor den underliggende behandling sker på grundlag af databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Danske Professionshøjskoler finder det samtidig hensigtsmæssigt, at eksemplerne tydeliggør, at loven fungerer som et supplerende retsgrundlag og ikke i sig selv etablerer hjemmel til den underliggende opgave eller behandling.

Begrebet ”borger”

Danske Professionshøjskoler foreslår, at begrebet ”borger” i § 3, stk. 1 erstattes med det mere generelle databeskyttelsesretlige begreb ”den registrerede”, eller at det i lovbemærkningerne præciseres, at bestemmelsen omfatter alle registrerede, herunder studerende, ansøgere, kursister, medarbejdere og forskningsdeltagere.

AI-genererede personoplysninger

Det fremgår af lovbemærkningerne til § 3, stk. 1, at bestemmelsen ikke kan anvendes som hjemmel til at behandle nye personoplysninger, men fungerer som supplerende retsgrundlag for behandling af personoplysninger, som myndigheden eller organet allerede behandler på grundlag af databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Danske Professionshøjskoler anbefaler, at det i lovbemærkningerne og det varslede vejledningsmateriale præciseres, om og på hvilke betingelser hjemlen omfatter generering og efterfølgende behandling af afledte personoplysninger, eksempelvis vurderinger, klassifikationer, anbefalinger og profiler, som ikke forelå før AI-behandlingen. Danske Professionshøjskoler finder en sådan afklaring væsentlig for lovens praktiske anvendelighed og for vurderingen af krav til blandt andet formålsbegrænsning, dataminimering, oplysningspligt og den registreredes rettigheder.

Forskning og udvikling

Danske Professionshøjskoler anbefaler, at lovbemærkningerne til § 3, stk. 1 tydeliggør samspillet mellem AI-hjemmelsloven, den underliggende hjemmel efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, og de eksisterende databeskyttelsesretlige regler om behandling til videnskabelige forskningsformål, herunder reglerne om behandling af særlige kategorier af personoplysninger. En sådan præcisering vil kunne mindske usikkerheden om, hvornår forsknings- og udviklingsaktiviteter er omfattet af loven, og hvornår behandlingen skal vurderes efter andre databeskyttelsesretlige regler.

Særlige kategorier af personoplysninger

Professionshøjskolerne behandler som led i deres opgaveløsning særlige kategorier af personoplysninger, eksempelvis helbredsoplysninger i forskning og oplysninger om specialpædagogisk støtte. Danske Professionshøjskoler anbefaler, at det i lovbemærkningerne til § 3, stk. 2 eller i det efterfølgende vejledningsmateriale tydeliggøres, hvornår eksisterende regulering på uddannelses- og forskningsområdet indeholder tilstrækkelige passende og specifikke foranstaltninger, og hvornår udvikling eller anvendelse af et AI-system, der behandler særlige kategorier af personoplysninger, forudsætter yderligere regulering.

Med venlig hilsen



Inge Friis Svendsen
Direktør
Danske Professionshøjskoler

Til Digitaliseringsstyrelsen

Sendt til digst@digst.dk og kopi til: jonmei@digst.dk, kahevi@digst.dk, emimol@digst.dk og leaomd@digst.dk

Danske Regioner

Høringssvar over forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

06-10-2026
EMN-2026-00222
1889097
Philip Lubertus Løfberg

Ved brev af 14. september 2026 har Digitaliseringsstyrelsen fremsendt udkast til lovforslag om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger. Danske Regioner afgiver hermed høringssvar på vegne af de fem regioner.

Generelle bemærkninger

Danske Regioner bakker overordnet positivt op om lovforslaget. Kunstig intelligens rummer et betydeligt potentiale for at frigøre tid til kerneopgaven, styrke kvaliteten og understøtte et mere digitalt sundhedsvæsen. Et klart retsgrundlag er derfor vigtigt for, at regionerne kan anvende teknologien ansvarligt og med respekt for borgernes og patienternes rettigheder.

Danske Regioner noterer sig samtidig, at lovforslaget alene vedrører anvendelse af AI-systemer til beslutningsstøtte, hvor et menneske fortsat indgår i beslutningsprocessen. Det er positivt, fordi menneskelig involvering kan understøtte både tilliden til anvendelsen af AI og fastholdelsen af sundhedspersonalets faglige kompetencer. Omvendt indebærer afgrænsningen, at lovforslaget ikke i samme grad understøtter de effektiviseringspotentialer, der kan være forbundet med mere autonome systemer, som kan varetage opgaver uden løbende menneskelig involvering.

I forhold til hjemmelsgrundlaget for anvendelse af AI til beslutningsstøtte lægger Danske Regioner til grund, at der efter en konkret vurdering allerede efter gældende ret kan være tilstrækkelig hjemmel til drift af visse AI-systemer. Det gælder navnlig, hvor anvendelsen ikke er indgribende, naturligt kan rummes inden for myndighedens eksisterende opgavevaretagelse, og de relevante sektorretlige, databeskyttelsesretlige og forvaltningsretlige krav er opfyldt. Lovforslaget kan dog på visse områder udgøre en relevant præcisering af det supplerende retsgrundlag og skaber hertil et tydeligt retsgrundlag med respekt for borgernes og patienternes rettigheder.

Bemærkninger til lovforslagets enkelte dele:
Nedenfor gennemgås lovforslagets enkelte bestemmelser i den rækkefølge, de fremgår af lovforslaget, med Danske Regioners konkrete bemærkninger til bestemmelserne og de tilhørende lovbemærkninger.

1. Lovens anvendelsesområde, jf. § 1

1.1. Myndigheds- og organbegrebet

Det følger af lovforslagets § 1, at loven gælder for alle offentlige myndigheder og organer, i det omfang de behandler personoplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, til opgaver, der udføres i samfundets interesse eller henhører under offentlig myndighedsudøvelse. Det fremgår af bemærkningerne, at begreberne "myndigheder" og "organer" skal forstås bredt og ikke er begrænset til afgrænsningerne i henholdsvis forvaltningsloven og udbudsloven, jf. lovforslagets side 14-15.

Danske Regioner hilser det brede anvendelsesområde velkommen. Det er væsentligt, at loven kan rumme den måde, den offentlige sektor og ikke mindst sundhedsvæsenet er organiseret på, hvor opgaver og digitale løsninger udvikles og anvendes på tværs af organisatoriske enheder.

Danske Regioner finder imidlertid, at lovbemærkningerne med fordel kan præcisere grænsen for, hvornår der ikke længere er tale om behandling inden for samme myndighed eller organ. Denne afgrænsning vil få væsentlig betydning efter lovforslaget. Det skyldes, at lovforslaget giver mulighed for at viderebehandle personoplysninger, som myndigheden eller organet allerede behandler, til udvikling af AI-systemer, hvorimod lovforslaget ikke giver hjemmel til at videregive oplysningerne til en anden myndighed eller et andet organ, jf. lovforslagets side 16-17.

Spørgsmålet er særligt relevant på sundhedsområdet, hvor udvikling og træning af AI-systemer kan ske på tværs af organisatoriske enheder. Muligheden for at anvende tilstrækkelige og relevante træningsdata kan have væsentlig betydning for udviklingen af AI-systemer.

Danske Regioner opfordrer derfor til, at lovbemærkningerne opstiller nærmere kriterier for denne vurdering, herunder eksempelvis organisatorisk placering og instruktionsbeføjelser. Det vil samtidig være hensigtsmæssigt at supplere bemærkningerne med konkrete eksempler fra sundhedsområdet, herunder hvor hospitaler, regionale fællesfunktioner og tværregionale samarbejder indgår i udviklingen eller træningen af samme AI-system.

2. Definitionerne i § 2

2.1. Beslutningsstøtte og "væsentlig indflydelse"

Det foreslås i lovforslagets § 2, nr. 4, at "beslutningsstøtte" defineres som forslag eller anbefalinger genereret af et AI-system, som en fysisk person inddrager i den samlede faglige vurdering, uden at AI-systemet selv træffer afgørelsen eller iværksætter tiltaget.

Det fremgår af lovbemærkningerne, at der ikke findes en generel definition af "beslutningsstøtte" i øvrig lovgivning, men samtidig anerkendes det, at begrebet allerede anvendes i konkrete sammenhænge på sundhedsområdet, jf. lovforslagets side 17-18 og 63. Det fremgår endvidere, at definitionen i lovforslaget skal kunne rumme den konkrete forståelse af begrebet, som allerede findes på sektorområder.

På sundhedsområdet forventes sundhedslovens § 48 e, stk. 3, imidlertid udmøntet i en bekendtgørelse, hvor der efter det foreliggende udkast indføres en særskilt definition af beslutningsstøtte. Her forstås beslutningsstøtte som *"støtte til en autoriseret sundhedsperson til at afveje fordele og ulemper af en given patientbehandling og på den baggrund træffe den bedst mulige sundhedsfaglige beslutning i en konkret og aktuel patientbehandlingssituation, herunder støtte til at stille en korrekt diagnose."*

Danske Regioner anbefaler derfor, at det konsekvent præciseres i lovbemærkningerne, at der ikke ses at være fastsat en "*generel definition*" af beslutningsstøtte i anden lovgivning. En sådan formulering vil både være mere præcis og give plads til eksisterende og kommende sektorspecifikke definitioner, herunder på sundhedsområdet.

Dette harmonerer samtidig med lovforslagets egen forudsætning om, at definitionen skal kunne rumme den forståelse af beslutningsstøtte, der allerede findes på

konkrete sektorområder, jf. lovforslagets side 63. Det vil efter Danske Regioners opfattelse være vigtigt for at undgå unødig tvivl om forholdet mellem den generelle definition i nærværende lovforslag og mere specifikke definitioner i sektorlovgivningen.

3. Udvikling og anvendelse efter § 3

3.1. Viderebehandling og historiske data

Det følger af lovforslagets § 3, stk. 1, at offentlige myndigheder og organer kan udvikle og anvende AI-systemer på baggrund af personoplysninger, som myndigheden eller organet allerede behandler, med henblik på at understøtte opgavevaretagelsen efter anden lovgivning. Bestemmelsen skal samtidig skabe grundlag for, at oplysninger, der oprindeligt er indsamlet til andre formål, kan viderebehandles til udvikling af AI-systemer uden en særskilt vurdering af formålenes forenelighed efter databeskyttelsesforordningens artikel 6, stk. 4, jf. lovforslagets side 70-71.

Adgangen omfatter efter bemærkningerne bl.a. personoplysninger fra historiske og lukkede sager. Det fremgår endvidere, at "udvikling" omfatter bl.a. træning, afprøvning, validering, gentræning og videreudvikling af AI-systemer, jf. lovforslagets side 65-66 og 69-71.

Danske Regioner hilser denne adgang velkommen. Muligheden for at anvende eksisterende oplysninger til udvikling og træning af AI-systemer er væsentlig for at kunne udvikle præcise og pålidelige løsninger, der efterfølgende kan anvendes som led i myndighedernes opgavevaretagelse.

Danske Regioner finder imidlertid, at denne adgang med fordel kan fremgå mere direkte af selve bestemmelsens ordlyd og ikke primært af lovbemærkningerne. Det bør således overvejes at præcisere i § 3, at eksisterende personoplysninger kan viderebehandles til bl.a. træning, afprøvning, validering, gentræning og videreudvikling af AI-systemer.

Endvidere finder Danske Regioner, at grænserne for viderebehandling af allerede opbevarede data skal tydeliggøres i lovforslagets bemærkninger, herunder at lovforslaget ikke ændrer på bl.a. reglerne om dataminimering og opbevaringsbegrænsning.

For regionerne er afgrænsningen særlig relevant i forhold til patientoplysninger og andre oplysninger, der er underlagt særlige sektorretlige regler om adgang og videregivelse. Lovforslaget fastslår, at § 3 ikke giver adgang til at indsamle yderligere personoplysninger, end myndigheden allerede efter gældende ret lovligt må indsamle og behandle, og at øvrige regler om anvendelse af oplysninger, herunder på sundhedsområdet, fortsat finder anvendelse, jf. lovforslagets side 71-72.

Danske Regioner anbefaler derfor, at det præciseres i bemærkningerne, hvilken betydning dette har for oplysninger, som myndigheden allerede lovligt har adgang til, eksempelvis oplysninger i patientjournaler. Regionerne behandler allerede sådanne oplysninger som led i patientbehandling, men det er uklart, om § 3 alene udgør hjemlen til at viderebehandle oplysningerne til det nye formål, dvs. udvikling af AI-systemet, eller om bestemmelsen også skal udgøre grundlaget for at indhente eller udtrække de relevante oplysninger fra journalsystemerne med henblik på denne viderebehandling.. En sådan præcisering vil gøre samspillet mellem AI-hjemmelsloven og de særlige regler om patientoplysninger væsentligt lettere at anvende i praksis.

3.2. Beslutningsstøtte, profilering og sundhedslovens § 48 e

Efter lovforslagets § 3, stk. 1, vil offentlige myndigheder og organer kunne udvikle og anvende AI-systemer, herunder til beslutningsstøtte og til evaluering af bestemte personlige forhold vedrørende en borger (profilering). Det fremgår samtidig af lovforslagets bemærkninger på side 16, at eksisterende sektorlovgivning på samme område fortsat skal finde anvendelse sideløbende med den foreslåede ordning.

På sundhedsområdet indeholder sundhedslovens § 48 e en hjemmel til behandling af personoplysninger til blandt andet beslutningsstøtte i forbindelse med patientbehandling. Det fremgår af forarbejderne, at bestemmelsen blandt andet skal muliggøre løbende træning af beslutningsstøtteværktøjer, herunder AI-modeller, og at bestemmelsen også omfatter personoplysninger, der tidligere er behandlet til videnskabelige og statistiske formål, herunder kvalitets- og forskningsprojekter, jf. § 48 e, stk. 2. Det fremgår imidlertid samtidig af forarbejderne, at det ved udmøntningen af bestemmelsen ikke er hensigten at fastsætte regler, der muliggør profilering af patienter, herunder profiler, som kan anvendes til beslutningsstøtte. Det er heller ikke hensigten, at oplysninger om en konkret person, som er behandlet i

et forskningsprojekt, efterfølgende skal kunne anvendes direkte over for den samme person.

Der kan derfor opstå tvivl om samspillet mellem lovforslagets generelle adgang til profilering efter § 3 og den sektorspecifikke regulering af beslutningsstøtte ved patientbehandling efter sundhedslovens § 48 e og regler fastsat i medfør heraf.

Danske Regioner foreslår på den baggrund, at det præciseres i lovbemærkningerne, hvordan § 3 skal anvendes i tilfælde, hvor et AI-system anvendes til klinisk beslutningsstøtte og samtidig indebærer profilering af patienten. Det bør navnlig præciseres, om § 3 er tilsigtet at give adgang til profilering i sådanne tilfælde, eller om behandlingen fortsat skal ske inden for rammerne af sundhedslovens § 48 e og regler fastsat i medfør heraf.

4. Passende og specifikke foranstaltninger jf. § 3, stk. 2

4.1. En positiv bevægelse fra "skal" til "kan"

Det følger af lovforslagets § 3, stk. 2, at vedkommende minister kan fastsætte regler om passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Danske Regioner ser positivt på, at bestemmelsen er formuleret som en adgang for vedkommende minister til at fastsætte sådanne regler og dermed som et "kan" frem for et "skal". Det giver mulighed for, at behovet for yderligere foranstaltninger vurderes konkret i stedet for, at der automatisk skal fastsættes supplerende regler i alle tilfælde. Der kan dermed tages højde for både risikoen ved den konkrete behandling og de garantier, , der allerede følger af databeskyttelsesforordningen, sektorlovgivningen samt konkrete tekniske og organisatoriske foranstaltninger.

Det bør imidlertid fremgå tydeligt af bemærkningerne, at der ikke gælder en formodning for, at der skal udstedes en bekendtgørelse, alene fordi et AI-system behandler oplysninger omfattet af databeskyttelsesforordningens artikel 9 eller 10. Behovet for yderligere regulering og garantier bør bero på en konkret vurdering af behandlingen, dens indgribende karakter, det anvendte retsgrundlag og de garantier, der allerede gælder.
Dette er efter Danske Regioners opfattelse særligt vigtigt i lyset af Datatilsynets praksis, som i flere tilfælde synes at indebære, at vurderingen af, om et supplerende retsgrundlag er tilstrækkeligt klart og præcist, i høj grad knyttes til selve den omstændighed, at der anvendes et AI-system. Datatilsynet har således haft en

praksis, hvor der ikke foretages en konkret vurdering af, om den konkrete behandlingsaktivitet og dens indgribende karakter betyder, at der er behov for at lave et supplerende retsgrundlag. Det er således alene den anvendte teknologi, som bliver afgørende herfor.

Hvis denne tilgang videreføres efter den foreslåede bestemmelse, er der efter Danske Regioners opfattelse en risiko for, at ændringen fra "skal" til "kan" reelt udvandes, fordi den tilsigtede fleksibilitet begrænses væsentligt i praksis. Det bør derfor præciseres i bemærkningerne, at selve anvendelsen af AI ikke i sig selv medfører krav om en bestemt reguleringsform, herunder udstedelse af en bekendtgørelse. Dette er også væsentligt i lyset af AI-systemers dynamiske karakter, som taler imod en tilgang, hvor anvendelsen af AI som teknologi i sig selv udløser krav om særskilt regulering.

5. Afsluttende bemærkninger

Danske Regioner bakker overordnet op om lovforslaget og anbefaler, at det gennemføres med de ovenfor anførte præciseringer. Det er væsentligt, at den endelige regulering fastholder en risikobaseret og teknologineutral tilgang og sikrer et klart og praktisk anvendeligt samspil med den eksisterende sektorlovgivning, herunder på sundhedsområdet.

Danske Regioner ser samtidig frem til det videre arbejde med rammerne for offentlig anvendelse af AI. Det gælder ikke mindst spørgsmålet om, hvorvidt og under hvilke rammer der fremover bør åbnes for mere automatiserede AI-systemer med mindre eller ingen løbende menneskelig involvering.

Digitaliseringsstyrelsen
Landgreven 4
1017 København K

DANSKE
UNIVERSITETER
UNIVERSITIES DENMARK

FIOLSTRÆDE 44, 1. TH
1171 KØBENHAVN K
TLF. +45 33 36 98 00
WWW.DKUNI.DK

12. OKTOBER 2026
ES

Høring over udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Danske Universiteter takker for ovennævnte udkast, som er modtaget i høring fra Uddannelses- og Forskningsstyrelsen den 14. september 2026.

Udkastet har været sendt i høring hos universiteterne. Danske Universiteter har modtaget svar fra Københavns Universitet, Aarhus Universitet, Syddansk Universitet og Danmarks Tekniske Universitet, der alle har sendt bemærkninger til udkastet. Bemærkninger er vedlagt.

Danske Universiteter støtter lovforslagets overordnede formål om at skabe et tydeligere og mere ensartet databeskyttelsesretligt grundlag for offentlige myndigheders udvikling og anvendelse af AI-systemer. Universiteterne ser et betydeligt potentiale i anvendelsen af AI til understøttelse af forskning, uddannelse, studieadministration og øvrige administrative opgaver og finder det vigtigt, at dette kan ske på et tydeligt og robust retligt grundlag.

Danske Universiteter har følgende overordnede bemærkninger:

Danske Universiteter finder, at lovforslagets anvendelsesområde med fordel kan præciseres yderligere. Det gælder blandt andet universiteternes status som offentlig myndighed efter loven, afgrænsningen af hvilke aktiviteter der er omfattet – det være sig forskning, uddannelse, studieadministration og/eller myndighedsudøvelse.

Der efterlyses større klarhed om samspillet mellem AI-hjemmelsloven, reglerne i databeskyttelsesloven og AI-forordningen, herunder hvordan loven skal anvendes i tilfælde, hvor AI-systemer understøtter flere formål eller anvendes på tværs af forskellige behandlingsgrundlag og opgaveområder. Der henvises til de vedlagte høringssvar for eksempler.

Danske Universiteter finder det væsentligt, at der sikres tydelige organisatoriske og styringsmæssige rammer for udvikling og anvendelse af AI-systemer. Dette gælder

blandt andet krav til dokumentation, sporbarhed, menneskeligt tilsyn, risikostyring, ansvar og kontrol.

Særligt bør der være tydeligt, hvordan lovens bestemmelser om beslutningsstøtte skal forstås og anvendes i praksis, og hvordan der sikres en ensartet tilgang til governance og kontrol ved forskellige typer af AI-anvendelser og risikoniveauer. Universiteterne peger på, at loven med fordel kan ledsages af nationale retningslinjer eller fælles standarder for AI-governance i den offentlige sektor, som ville give tydelig retning.

Universiteterne vurderer, at lovforslagets værdi vil afhænge af, at offentlige myndigheder og organer får adgang til fælles, praksisnære og sektorrelevante vejledninger. Universiteterne noterer sig derfor positivt, at Digitaliseringsstyrelsen planlægger yderligere vejledning. Universiteterne ser særligt behov for praksisnære fortolkningsbidrag om lovens anvendelsesområde, samspillet med eksisterende regulering, krav til menneskeligt tilsyn samt governance- og kontrolrammer ved udvikling og anvendelse af AI-systemer.

Der henvises til vedlagte høringssvar fra universiteterne for individuelle bemærkninger til udkastet.

Med venlig hilsen

Jesper Langergaard
Direktør
Danske Universiteter

KØBENHAVNS UNIVERSITET

Til:
Danske Universiteter
Forsknings-, Uddannelses- og Digitaliseringsministeriet

Vedrørende høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

7. oktober 2026

KU Forskning og Informationssikkerhed
Forskningsservice og Udvikling

Nørregade 10
København K

DIR 35 33 01 41
MOB 51 30 25 86

niko@adm.ku.dk

Københavns Universitet takker for muligheden for at afgive høringssvar vedr. AI-hjemmelsloven.

Københavns Universitet kan oplyse, at universitetet støtter lovforslagets overordnede formål om at skabe et klarere, ensartet og fremtidssikret databeskyttelsesretligt grundlag for offentlige myndigheders og organers udvikling og anvendelse af AI-systemer. En tydelig hjemmel vil kunne reducere den retlige usikkerhed, som i dag kan vanskeliggøre ansvarlig udvikling og implementering af AI i den offentlige sektor.

For Københavns Universitet er der et betydeligt potentiale i AI. AI-systemer kan blandt andet understøtte uddannelse, studieadministration, vejledning, forskning, forskningsadministration, HR, IT-drift og informationssikkerhed og andre administrative processer. Universitetet finder det væsentligt, at lovgivningen både gør det muligt at realisere dette potentiale og sikrer, at brugen sker på et tydeligt, forudsigeligt og databeskyttelsesretligt robust grundlag som er gennemskueligt for universitetets mange registrerede.

Bemærkninger til § 1

Det er positivt, at lovforslaget etablerer en generel databeskyttelsesretlig hjemmel til udvikling og anvendelse af AI-systemer ved behandling af personoplysninger, når behandlingen sker som led i opgaver i samfundets interesse eller offentlig myndighedsudøvelse, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e. Det er ligeledes

positivt at den seneste version af bestemmelsen indeholder en komplet henvisning til artikel 6, stk. 1, litra e i sin ordlyd.

Bemærkninger til § 3

- Københavns Universitet finder det positivt at loven omfatter udvikling, således at hele AI-systemets livscyklus er omfattet af loven og ikke kun slutproduktet.
- Københavns Universitet finder, at det med fordel kan tydeliggøres, hvorvidt § 3 skal forstås således, at den alene er en behandlingshjemmel til anvendelse af AI som led i opgaver, som den pågældende myndighed eller det pågældende organ allerede har hjemmel eller pligt til at varetage efter anden lovgivning. At § 3 derfor ikke kan anvendes som selvstændigt grundlag for at foretage ny indsamling af personoplysninger, etablere nye offentlige opgaver, nye kompetencer eller nye afgørelsesbeføjelser.
- Københavns Universitet finder, at det med fordel kan ekspliciteres, om § 3 kan bruges som hjemmel til at forlænge opbevaringsperioden for personoplysninger alene når det er med henblik på udvikling, afprøvning, validering, gentræning eller videreudvikling af et AI-system. Herunder om personoplysninger, herunder kopier, udtræk og datasæt til træning, test eller validering, må opbevares længere end efter den øvrige behandlingshjemmel og reglerne for den oprindelige behandling.
- Københavns Universitet finder, at det med fordel kan præciseres, om § 3 kan anvendes som supplerende retsgrundlag, når to eller flere offentlige myndigheder eller organer i fællesskab udvikler, træner, afprøver, validerer, gentræner eller ibrugtager et AI-system. Det bør i den forbindelse tydeliggøres, om hver myndighed eller hvert organ kan bidrage med personoplysninger, som myndigheden eller organet selv lovligt behandler, og om et fælles AI-system efterfølgende kan anvendes af de deltagende myndigheder og organer til deres respektive fastlagte og afgrænsede opgaver. Det ønskes oplyst, om bestemmelsen kan anvendes ved et samarbejde mellem flere universiteter eller andre offentlige organer, hvor hver deltager bidrager med personoplysninger som denne er dataansvarlig for til udvikling og træning af et fælles AI-system, forudsat at hver deltager har hjemmel til den oprindelige behandling, og at systemet alene anvendes til deltagernes respektive fastlagte og afgrænsede opgaver.

Særligt ift. § 3 og forskning

- Forholdet imellem AI-hjemmelsloven § 3 og Databeskyttelseslovens § 10 fremstår uklart. Mens det jfr. AI-hjemmelslovens § 3 fremstår for Københavns Universitet således, at denne lov giver hjemmel til anvendelse af AI-systemer både som redskab og genstand for forskningen, når det drejer sig om almindelige personoplysninger (cf. AI-hjemmelslovens § 1), så fremstår det uklart om AI-hjemmelslovens § 3 også kan anvendes som hjemmel til forskning i følsomme personoplysninger og oplysninger om strafbare forhold, der er hjemlet i databeskyttelseslovens § 10, med henvisning til både artikel 6 (retlig basis), artikel 9 (undtagelse til forbud mod behandling af følsomme personoplysninger) og artikel 10 (ang. krav til behandling af oplysninger om strafbare forhold), eller om det er en forudsætning herfor at der sker aktivering på ressortområdet jfr. § 3 stk. 2.
- I fald behandling af følsomme personoplysninger og oplysninger om straffeforhold kræver aktivering jfr. § 3, stk. 2 imødeser Københavns Universitet gerne aktivering via bekendtgørelse dækkende for forskningsområdet.
- Københavns Universitet finder, at forholdet mellem AI-hjemmelslovens § 3, databeskyttelseslovens § 10 og forskningsbaserede behandlingsgrundlag bør tydeliggøres. Efter lovforslagets § 1 og § 3 er bestemmelsen afgrænset til behandlinger, der sker med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, som led i en allerede fastlagt og afgrænset opgavevaretagelse efter andet retsgrundlag.

  Københavns Universitet finder således, at det bør præciseres, at § 3 ikke via sin udeladelse udgør et modsætningsvist forbud mod anvendelse af AI-systemer, når behandlingen er hjemlet efter andre behandlingsgrundlag, herunder databeskyttelsesforordningens artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a om udtrykkeligt samtykke.

  Dette er særligt relevant for forskning, herunder internationale forskningssamarbejder, hvor samtykke ofte anvendes som behandlingsgrundlag. I store databaser vil der ofte være personoplysninger, der er indsamlet på forskellige behandlingsgrundlag, fx på baggrund af samtykke efter artikel 6, stk. 1, litra a og artikel 9, stk. 2, litra a, og efter anden lovgivning, fx

artikel 6, stk. 1, litra e. Det kan i praksis være vanskeligt at adskille de enkelte oplysninger efter deres respektive behandlingsgrundlag.

Denne blanding af behandlingsgrundlag vanskeliggør samtidig håndteringen af den registreredes rettigheder, idet den registreredes rettigheder ikke vil være begrænset efter lovforslagets § 4, når det juridiske grundlag for behandlingen er samtykke.

Generelt

Universitetet noterer sig positivt, at Digitaliseringsstyrelsen planlægger yderligere vejledning.

Det bør tydeliggøres i bemærkningerne til § 3, at hjemmel til behandling af personoplysninger ved anvendelse af AI ikke i sig selv betyder, at data er egnede til AI-behandling.

Lovforslagets praktiske værdi vil i høj grad afhænge af, om myndigheder og organer får adgang til fælles, praksisnære og sektorrelevante fortolkningsbidrag. Universiteterne har komplekse og forskellige opgaver, og vil imødese vejledning der vil kunne understøtte både innovation og ensartet efterlevelse inden for sektoren.

Med venlig hilsen på vegne af Københavns Universitet
Nicklas Jakobsen
Fuldmægtig, KU Forskning og Informationssikkerhed, Københavns Universitet

Godkendt af:
Kim Brinckmann
Vicedirektør, KU Forskning og Informationssikkerhed, Københavns Universitet

AARHUS UNIVERSITET

Danske Universiteter
Fiolstræde 44, 1. th
1171 København K

Bemærkninger til høring om AI-hjemmelsloven

Informationssikkerhed

Loa Skau Björnsson
Jurist

Dato: 5. oktober 2026

Mobiltlf.: +4551715375
E-mail: loaskau@au.dk
Web: au.dk/loaskau@au.dk

Afs. CVR-nr.: 31119103

Aarhus Universitet (AU) behandler en lang række personoplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, herunder i forbindelse med forskning, uddannelse, myndighedsbetjening og personaleadministration.
AU har derfor en væsentlig interesse i at kunne anvende AI-systemer til blandt andet beslutningsstøtte og effektivisering af opgavevaretagelsen og hilser lovforslagets formål om at etablere et generelt databeskyttelsesretligt retsgrundlag for offentlige myndigheders og organers udvikling og anvendelse af AI-systemer velkommen.

Generelle bemærkninger

Lovforslaget tillægger flere steder vedkommende minister kompetence til at fastsætte regler eller foranstaltninger, når der opstår et behov i forbindelse med en myndigheds udvikling eller anvendelse af AI-systemer.
Det er imidlertid uklart, hvordan et sådant behov skal bringes til ministerens kendskab, og hvilken proces der herefter skal følges. Det fremgår således ikke klart, om den enkelte myndighed forventes at orientere ministeren, eller om bemyndigelserne alene anvendes på ministerens eget initiativ. Det er ligeledes uklart, hvordan myndigheden skal forholde sig til en planlagt eller igangværende behandling, mens spørgsmålet afklares.
AU anbefaler derfor, at processen tydeliggøres, navnlig i relation til § 3, stk. 2, og § 4, stk. 1. Manglende klarhed kan skabe retlig og praktisk usikkerhed og indebære økonomiske konsekvenser for myndigheder, som udvikler eller anvender AI-systemer.

Bemærkninger til § 2, nr. 4 – definitionen af beslutningsstøtte

AU finder, at definitionen af beslutningsstøtte med fordel kan præciseres yderligere. Bemærkningerne indeholder en række eksempler, men efterlader fortsat en vis usikkerhed om navnlig forståelsen af "væsentlige tiltag" og "væsentlig indflydelse på sagsbehandlingens forløb" samt sondringen mellem almindelig AI-assisteret sagsforberedelse, beslutningsstøtte og automatiserede afgørelser.

AU anbefaler derfor, at afgrænsningen tydeliggøres, fx gennem yderligere konkrete eksempler i lovbemærkningerne, så reglerne kan anvendes mere ensartet.

Informationssikkerhed
Aarhus Universitet
Universitetsbyen 81
8000 Aarhus C

Tlf.: +45 8715 2946
E-mail: it@au.dk
Web: https://medarbejdere.au.dk/administration/administration/au-it/informationssikkerhed/

Bemærkninger til § 3, stk. 2

Efter § 3, stk. 2, kan vedkommende minister på eget ressort fastsætte passende og specifikke foranstaltninger ved behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10.

Samtidig forudsætter lovbemærkningerne, at den dataansvarlige myndighed som led i sine databeskyttelsesretlige vurderinger identificerer nødvendigheden af behandlingen og relevante beskyttelsesforanstaltninger, herunder som led i en konsekvensanalyse efter databeskyttelsesforordningens artikel 35.

Det er imidlertid ikke beskrevet, hvordan myndighedens vurdering kobles til ministerens kompetence efter § 3, stk. 2. AU anbefaler derfor, at det præciseres, hvordan og hvornår et identificeret behov forventes bragt til ministerens kendskab, og om behandlingen kan påbegyndes eller fortsættes, mens spørgsmålet afklares. Dette er særligt relevant for AI-systemer udviklet til konkrete eller lokale behov, som ministeren ikke nødvendigvis har kendskab til.

AI-systemer, der berører flere ressortområder

AU hører organisatorisk under ét ministerområde, men varetager opgaver, der kan berøre flere ministeriers ressortområder.

Det bør derfor præciseres, hvilken minister der har kompetencen efter § 3, stk. 2, når et AI-system berører flere ressortområder, herunder hvilke regler der gælder, hvis de relevante ressortministre ikke udsteder en fælles bekendtgørelse.

Konsekvenser ved efterfølgende krav

En myndigheds egen udvikling og implementering af AI-systemer kan indebære betydelige investeringer, herunder til træning af AI-systemet og uddannelse af medarbejdere. Hvis ministeren efterfølgende fastsætter nye eller supplerende krav efter § 3, stk. 2, kan det nødvendiggøre væsentlige tekniske eller organisatoriske ændringer, der kan medføre betydelige meromkostninger for myndigheden og i yderste konsekvens medføre, at anvendelsen af AI-systemet må ophøre.

AU anbefaler derfor, at processen og tidspunktet for anvendelsen af bemyndigelsen efter § 3, stk. 2 tydeliggøres, så myndigheder på et tilstrækkeligt tidligt tidspunkt kan opnå klarhed over de krav, der gælder for en planlagt behandling.

Bemærkninger til § 4

Efter § 4, stk. 1, kan vedkommende minister fastsætte regler om begrænsning af visse af de registreredes rettigheder, hvis betingelserne i databeskyttelsesforordningens artikel 23 er opfyldt.

AU finder det uklart, i hvilke situationer og efter hvilken proces denne bemyndigelse forventes anvendt. Det gælder navnlig, hvis en myndighed i forbindelse med et konkret AI-system identificerer forhold, som kan begrunde, at ministeren overvejer at fastsætte regler efter § 4, stk. 1.

AU anbefaler derfor, at det præciseres, om myndigheden i sådanne tilfælde kan eller skal rette henvendelse til vedkommende minister, og hvordan myndigheden skal forholde sig til behandlingen, indtil spørgsmålet er afklaret.
Mere generelt bør det således fremgå tydeligt, hvordan den enkelte myndighed forventes at reagere, når den identificerer et behov, der kan være omfattet af bemyndigelserne i § 3, stk. 2, eller § 4, stk. 1.

Forholdet til øvrige regler om indsigt og aktindsigt
AU modtager jævnligt anmodninger om indsigt efter databeskyttelsesforordningens artikel 15. Den registrerede kan samtidig have ret til adgang til de samme eller overlappende oplysninger efter andre regelsæt, herunder de forvaltningsretlige regler om aktindsigt.
Det fremgår af lovbemærkningerne, at § 4, stk. 1, ikke ændrer krav i anden lovgivning. AU anbefaler derfor, at det tydeliggøres, hvilken praktisk betydning en begrænsning efter § 4, stk. 1, har, hvis den registrerede fortsat kan få adgang til de samme eller i det væsentlige overlappende oplysninger efter andre regelsæt.

Venlig hilsen

Loa Skau Björnsson
Jurist

Danske Universiteter
E-mail: dkuni@dkuni.dk

SDU's bidrag til Danske Universiteters samlede høringssvar vedr. AI-hjemmelsloven

Dato: 6. oktober 2026

Sagsnr. 26/59652

SDU takker hermed for muligheden for at indsende bemærkninger til ovennævnte høring.

SDU bemærker følgende:

1. Det ønskes præciseret, hvorvidt universiteter omfattet af universitetsloven anses for "offentlige myndigheder eller organer" efter lovforslaget, og i hvilket omfang universiteternes aktiviteter inden for forskning, uddannelse, studieadministration og myndighedsudøvelse er omfattet af lovens anvendelsesområde.

2. Hvordan forholder ministeriet sig til offentlige myndigheders og universiteters behandling baseret på art. 6, stk. 1, litra c, når disse behandlinger udgør en integreret del af myndighedens lovbestemte opgavevaretagelse, og AI-systemer anvendes på tværs af processer, der hviler på både art. 6, stk. 1, litra c og e?

   Vil det være muligt at præcisere i bemærkningerne, hvordan offentlige myndigheder og universiteter skal håndtere AI-anvendelser ved behandlinger baseret på artikel 6, stk. 1, litra c? Uden en sådan præcisering risikerer lovforslaget at skabe ny usikkerhed om anvendelse af AI i offentlige myndigheders lovbundne opgavevaretagelse.

3. Skal hele universitetslovens formål forstås som "opgavevaretagelse", eller skal der foretages en snævrere vurdering?

   Hvordan skal AI-hjemmelsloven forstås i tilfælde, hvor samme AI-system anvendes til flere formål samtidig, herunder forskning, uddannelse,

Syddansk Universitet
Campusvej 55
5230 Odense M
T +45 6550 1000
www.sdu.dk

studieadministration og myndighedsudøvelse? Et studieadministrativt AI-system kan samtidig trænes på historiske sager, bruges i uddannelseskvalitet, analyseres forskningsmæssigt og understøtte myndighedsafgørelser.

4. Lovforslaget forudsætter, at en række anvendelser af AI til beslutningsstøtte kan ske på grundlag af den generelle hjemmel. Mange af disse anvendelser må forventes samtidig at kunne være omfattet af AI-forordningens regler om højrisiko-AI-systemer. Det ønskes derfor præciseret, hvordan ministeriet ser samspillet mellem lovforslagets hjemmel og de krav til risikostyring, menneskeligt tilsyn, dokumentation og kontrol, der følger af AI-forordningen.

5. Lovforslaget bygger på en sektorvis model, hvor ressortministrene kan fastsætte passende og specifikke foranstaltninger ved behandling af personoplysninger efter databeskyttelsesforordningens artikel 9 og 10. Det fremgår imidlertid ikke, hvordan der sikres ensartethed og sammenhæng på tværs af ressortområderne. Der savnes derfor en nærmere beskrivelse af, hvilke mekanismer der skal sikre et ensartet beskyttelsesniveau for registrerede på tværs af den offentlige sektor, herunder ved fællesoffentlige eller tværgående AI-løsninger.

6. Lovforslaget bygger på en sondring mellem beslutningsstøtte og automatiserede individuelle afgørelser, hvor afgørende betydning tillægges reel menneskelig involvering. Samtidig anføres det i bemærkningerne, at kravet til graden af menneskelig involvering ikke er klart fastlagt i praksis. Det ønskes derfor præciseret, hvilke konkrete kriterier der efter ministeriets opfattelse skal være opfyldt, for at menneskelig kontrol kan anses for reel og meningsfuld ved anvendelse af AI-systemer til beslutningsstøtte, og hvordan automation bias skal håndteres i praksis.

7. Er det muligt at inddrage specifikke universitetseksempler i forarbejderne? F.eks. scenarier vedr. punkt 3, eller når et AI-system f.eks. udvikles som led i en forskningsaktivitet, men efterfølgende ønskes anvendt i universitetets myndighedsudøvelse eller studieadministration.

Med venlig hilsen

Ida Marie Hansen
Jurist, SDU RIO Legal Services

Janni Brodersen
Informationssikkerhedschef
Leder af Governance, Risk & Compliance, SDU IT

Høringssvar fra DTU

Høringssvar vedrørende forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Offentlige organisationer har behov for klare rammer for ansvarlig anvendelse af AI, herunder til beslutningsstøtte, administrative processer og forbedring af eksisterende arbejdsgange. Lovforslaget kan bidrage til at reducere retlig usikkerhed og understøtte digital innovation i den offentlige sektor.

DTU vurderer samtidig, at lovforslaget bør suppleres med stærkere krav til governance, dokumentation, sporbarhed, bias-kontrol, audit og beskyttelse af registreredes rettigheder

Behov for tydeligere nationale governance-rammer

Lovforslaget etablerer et behandlingsgrundlag, men adresserer kun i begrænset omfang de organisatoriske og styringsmæssige udfordringer, som følger af anvendelsen af AI-systemer.

Udvikling og anvendelse af AI rejser spørgsmål om:

- dokumentation,
- sporbarhed,
- menneskeligt tilsyn,
- løbende kontrol,
- ansvar og governance.

DTU anbefaler derfor, at loven ledsages af nationale retningslinjer eller fælles standarder for AI-governance i den offentlige sektor.

Dette vil understøtte en ensartet praksis på tværs af myndigheder og reducere risikoen for forskellige fortolkninger af lovens rammer.

Risikobaseret regulering bør understøttes tydeligere

DTU finder det vigtigt, at den praktiske implementering af loven sker efter en risikobaseret tilgang i overensstemmelse med AI-forordningens grundlæggende principper.

Der bør være en tydelig forskel mellem:

- AI-løsninger, der anvendes til administrative støttefunktioner,

- og AI-systemer, der anvendes til vurdering af personer, profilering eller beslutningsstøtte med potentiel betydning for den registrerede.

Det kan derfor overvejes, om lovforslaget eller tilhørende vejledninger tydeligere bør beskrive forventningerne til governance, dokumentation og kontrol ved forskellige risikoniveauer.

Anvendelse af historiske data

DTU ser positivt på, at lovforslaget søger at skabe klarhed om mulighederne for at anvende allerede lovligt indsamlede personoplysninger til udvikling af AI-systemer. Dette kan understøtte udviklingen af mere præcise og relevante AI-løsninger baseret på organisationernes egne proces- og sagsdata.

Samtidig anbefales det, at der udarbejdes nærmere vejledning om:

- anvendelsen af historiske data,
- proportionalitetsvurderinger,
- dataminimering,
- anonymisering og pseudonymisering,
- samt dokumentation af de databeskyttelsesretlige vurderinger.

Dette vil styrke tilliden til anvendelsen af AI-systemer baseret på historiske datasæt.

Forholdet til AI-leverandører

DTU finder det væsentligt, at der skabes større klarhed om ansvarsfordelingen mellem offentlige myndigheder og leverandører af AI-systemer.

Særligt bør der gives yderligere vejledning om:

- anvendelse af data hos leverandører,
- brug af underdatabehandlere,
- modeltræning hos leverandøren,
- tredjelandsoverførsler,
- samt håndtering af fejl og bias.

Dette vurderes at være et af de områder, hvor mange af de væsentlige praktiske risici opstår ved implementering af AI-løsninger.

Fremtidige AI-agenter og autonome funktioner

Lovforslaget tager udgangspunkt i AI-systemer generelt, men udviklingen bevæger sig mod mere autonome AI-agenter, som ikke alene genererer indhold, men også kan udføre handlinger på tværs af systemer.

DTU anbefaler derfor, at kommende vejledninger eller bekendtgørelser adresserer behovet for:

- logning,
- revisionsspor,
- rolle- og adgangsstyring,
- transparens,
- og ansvar ved automatiserede handlinger udført af AI-systemer.

Disse spørgsmål forventes at få stigende betydning i de kommende år.

Afslutning

DTU støtter den overordnede ambition om at etablere et generelt og mere klart retsgrundlag for offentlige myndigheders udvikling og anvendelse af AI-systemer ved behandling af personoplysninger. Lovforslaget kan bidrage til at reducere den retlige usikkerhed, som i dag kan hæmme ansvarlig innovation og digitalisering i den offentlige sektor.

DTU anbefaler samtidig, at lovforslaget suppleres med tydeligere rammer for governance, dokumentation, menneskelig kontrol, ansvar og sporbarhed, således at innovation og effektivisering understøttes inden for robuste og tillidsskabende rammer for databeskyttelse og retssikkerhed.

Sekretariatet for
Dataetisk Råd
dataetiskraad.dk
dataetiskraad@dketik.dk

Dato: 12.10.2026

Digitaliseringsstyrelsen
Sendt elektronisk til jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk, og kahevi@digst.dk.

Dataetisk Råds høringssvar til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

1. Introduktion

Dataetisk Råd takker for den fremsendte høring. Dataetisk Råd er en offentlig myndighed som rådgiver den offentlige og private sektor, den danske offentlighed samt Regeringen og Folketinget om dataetiske problemstillinger knyttet til nye digitale teknologier, inklusiv kunstig intelligens (AI). Rådets formål er at støtte etisk udvikling og anvendelse af disse teknologier, dertil at rådgive om den regulering, der kan skabe de relevante rammer for dette.

Rådet forstår at formålet med lovforslaget er, at give offentlige myndigheder, samt visse andre organer, en bred og almen hjemmel, til at udvikle og anvende AI, herunder især hjemmel til at anvende personoplysninger til træning og under brug, og til at lade AI udføre beslutningsstøtte for myndighederne. Forslaget udvider således ikke myndigheders mulighed for at indhente eller dele data, men giver myndigheder øgede muligheder for at behandle data, som myndigheden allerede har adgang til, med det specifikke formål at udvikle og anvende AI.

Det er Dataetisk Råds forståelse, at forslaget er motiveret af i) at Databeskyttelsesretten stiller krav om en sådan hjemmel, samt ii) at der for de fleste myndigheder i dag ikke findes en sådan hjemmel i dansk lovgivning, hvilket iii) hidtil har begrænset offentlige myndigheders muligheder for at udvikle og anvende AI. Alternativet til den foreslåede brede og almene hjemmel er således at de relevante myndigheder gives hjemmel gennem love eller bekendtgørelser målrettet den individuelle myndighed og/eller den konkrete anvendelse, eller at disse myndigheder undlader at anvende AI på de tilsigtede måder.

I tilknytning til den brede og almene hjemmel, som lovforslaget etablerer, gives resortministrene mulighed for at fastsætte foranstaltninger til beskyttelse af personers rettigheder ved behandling af særligt følsomme personoplysninger, når dette efter databeskyttelsesretten er nødvendigt.

Endelig giver loven resortministrene mulighed for i visse tilfælde at indføre undtagelser til de rettigheder, som personer normalt nyder under databeskyttelsesretten i forbindelse med udvikling og anvendelse af AI, eksempelvis retten til indsigt, indsigelse, berettigelse og sletning. Det fremføres i bemærkningerne til lovforslaget, at muligheden for at indføre disse undtagelser motiveres af, at det i nogle situationer vil være teknisk vanskeligt for myndigheder eksempelvis at give indsigt i hvordan persondata er anvendt til træning af en model, eller at ændre på en model, som under udviklingen har anvendt persondata, der ønskes slettet.

1.1 Dataetisk Råds overordnede anbefalinger

Dataetisk Råd har i foråret 2026 fremsendt høringssvar på en tidligere version af lovforslaget. Dataetisk Råds bemærkninger genfremsendes i let justeret form, idet det er rådets vurdering, at ændringerne i det genfremsatte lovforslag i begrænset omfang imødekommer de anbefalinger, som rådet fremsatte i forbindelse med det allerede afgivne høringssvar.

Dataetisk Råds arbejde i vurderingen af dataetiske spørgsmål tager udgangspunkt i tre overordnede og ni underordnede dataetiske principper.[1] Rådet anerkender de mange potentielle fordele ved at anvende kunstig intelligens i den offentlige forvaltning. Som det fremføres i lovforslagets bemærkninger kan anvendelsen potentielt effektivisere myndighedernes arbejde, og derved frigive ressourcer og/eller reducere behandlingstiden, samt øge ensartethed og/eller kvalitet i myndighedsarbejdet.

Samtidig vurderer rådet at lovforslaget rejser betydelige dataetiske udfordringer, herunder særligt i tilknytning til de overordnede principper om at gøre gavn, ikke skade og at sikre retfærdighed, samt de underordnede principper om privatliv, velfærd, ansvarlighed, retssikkerhed, lighed og forklarlighed. Rådet anbefaler i den forbindelse

i) udvidelse af hjemmel til systemer som er beslægtet med den anførte definition af AI,
ii) præcisering af definitionen af beslutningsstøtte,
iii) eksplicit afgrænsning af hjemmel til fuldt automatiserede beslutninger,
iv) indførelse af generelle minimumsstandarder for beskyttelse af følsomme persondata,
v) begrænsning af undtagelser til registreredes rettigheder,
vi) etablering af retningslinjer for kvalitetssikring, samt
vii) udførelse af en dataetisk konsekvensanalyse for lovforslaget.

Endelig og mest centralt anbefaler Dataetisk Råd

viii) at Regering og Folketing overvejer, om det samlet set er hensigtsmæssigt, at etablere en bred og almen hjemmel, givet at der fortsat er begrænsede retningslinjer for og erfaringer med hvordan offentlige myndigheder etisk kan anvende AI til

[1] https://www.dataetiskraad.dk/dataetiske-temaer/hvad-er-dataetik/dataetiske-principper

beslutningsstøtte, samt at en sådan hjemmel i modsætning til specifikke hjemler målrettet den individuelle myndighed og/eller den konkrete anvendelse gør det vanskeligt at vurdere risici og nødvendige forholdsregler. Ved at lovfæste en bred og almen hjemmel mister Regering og Folketing således muligheden for i de enkelte tilfælde at tage stilling til, om der bør udstedes hjemmel til den konkrete anvendelse, herunder muligheden for at indhente høringssvar, som kan belyse fordele og ulemper, samt indføre målrettede rammer og betingelser for den konkrete anvendelse.

2. Bemærkninger til lovforslaget

2.1. Udvidelse af hjemmel til AI-beslægtede systemer (§ 2, stk.1)

Forslaget tager udgangspunkt i AI-forordningens definition af AI, idet et AI-system defineres som: "et maskinbaseret system, som er udformet med henblik på at fungere med en varierende grad af autonomi, og som efter idriftsættelsen kan udvise en tilpasningsevne, og som til eksplicitte eller implicitte mål af det input, det modtager, udleder, hvordan det kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer." Anvendelsen af denne definition motiveres af, at loven dermed bringes i overensstemmelse med forordningen, og kan trække på den udvikling i fortolkningen, som forventeligt vil finde sted i regi af forordningen.

Dataetisk Råd skal hertil bemærke, at der er tale om en kompleks, teknisk definition, som kan være vanskelig at anvende. Dertil kommer, at definitionen bevidst udelukker visse enkle computersystemer til vurderinger og beslutningsstøtte, som ikke jf. definitionen kan klassificeres som AI. Loven vil således ikke give hjemmel til udvikling og anvendelse af systemer som behandler persondata for at generere et output såsom forudsigelser, indhold, anbefalinger eller beslutninger, i) hvis et sådant system ikke er udformet med henblik på at fungere med en varierende grad af autonomi,[2] ii) hvis systemet ikke kan udvise tilpasningsevne efter idriftsættelsen, eller iii) hvis det skabte output ikke kan påvirke fysiske eller virtuelle miljøer. Det er rådets opfattelse, at mange af de systemer til algoritmisk beslutningsstøtte, som offentlige myndigheder historisk har brugt, og fremadrettet kunne ønske at bruge, ikke vil kunne klassificeres som AI jf. denne definition, fordi de enten ikke er designet til at fungere autonomt, ikke er tilpasningsdygtige, eller ikke selvstændigt påvirker fysiske eller virtuelle miljøer.

[2] Rådet fortolker formuleringen i denne del af definitionen således, at systemer som har en vis, tilstrækkelig grad af autonomi (snarere end "varierende autonomi") forstås som AI, samt at definitionen omfatter systemer som faktisk har en vis, tilstrækkelig grad af autonomi uanset om de er udformet med henblik på dette, men omvendt ikke omfatter systemer, som er udformet med et sådant henblik, men som i praksis ikke har den relevante form for autonomi.

Definitionen medfører således at der kan opstå situationer, hvor en myndighed teknisk har mulighed for at udvikle og anvende et enkelt, letforståeligt og billigt system til automatiseret beslutningsstøtte, men savner hjemmel til dette, fordi systemet ikke kan klassificeres som AI, hvorfor myndigheden i stedet må udvikle og anvende et mere komplekst, uigennemskueligt og omkostningstungt AI-system.

Dataetisk Råd anbefaler i lyset af det dataetiske princip om forklarlighed, for så vidt Regeringen og Folketinget ønsker at give myndigheder en bred og almen hjemmel til udvikling og anvendelse af AI, at hjemlen udvides, således at der i tillæg til hjemmel til egentlige AI-systemer jf. forordningens definition, også gives hjemmel til mere enkle, AI-lignende systemer, herunder regelbaserede systemer og enkle maskinlærte modeller. Derved sikres, at myndigheder juridisk set har lige så gode muligheder for at benytte enkle systemer til automatiseret beslutningsstøtte, som de har for at benytte mere komplekse AI-systemer.

2.2. Præcisering af forslagets definition af beslutningsstøtte (§ 2, stk.4)

Den foreslåede lov giver offentlige myndigheder hjemmel til udvikling og brug af AI til blandt andet beslutningsstøtte. Forslagets bemærkninger påpeger, at "beslutningsstøtte" ikke er veldefineret, og indfører definitionen, at beslutningsstøtte ifm. loven skal forstås som: "enhver form for forslag eller anbefaling til afgørelser eller væsentlige tiltag overfor den registrerede, som er genereret af et AI-system, og som en fysisk person inddrager i den samlede faglige vurdering, som ligger til grund for afgørelsen eller tiltaget, uden at AI-systemet selv træffer afgørelse eller iværksætter tiltaget."

Dataetisk Råd bemærker, at beslutningsstøtte i faglitteraturen ofte forstås bredere, således at ikke blot "forslag eller anbefalinger om afgørelser eller tiltag", men også eksempelvis udledning af faktuelle vurderinger, som indgår i et beslutningsgrundlag, kan udgøre beslutningsstøtte. Den foreslåede definition forekommer i denne forbindelse at være snævrere end tilsigtet.

Forslaget gør i bemærkningerne opmærksom på, at det kan være vanskeligt at trække grænsen mellem beslutningsstøtte og fuldt automatiserede beslutninger. Forslagets definition af beslutningsstøtte lægger i udgangspunktet op til en fortolkning, hvor fuldt automatiserede beslutninger alene forstås som den situation, hvor et AI-system selv træffer en afgørelse eller iværksætter et tiltag, dvs. uden nogen grad af menneskelig involvering. I faglitteraturen defineres beslutningsstøtte ofte snævrere, som situationer hvor en menneskelig beslutningstager har "meningsfuld kontrol" med beslutningen. Denne definition forudsætter en yderligere præcisering af hvornår menneskelig kontrol er meningsfuld. Bemærkningerne til forslaget fremfører tilsvarende, at "…menneskelig involvering skal omfatte en reel stillingtagen til eller vurdering af AI-systemers anbefalinger og forslag, førend der er tale om "beslutningsstøtte"", således at " menneskelig involvering i så ringe en grad, at det alene anses som en formalitet, ikke vil kunne anses som beslutningsstøtte…" Forslaget udskyder imidlertid en præcisering til fremtidig afklaring i forbindelse med udvikling af retspraksis på området.

Det er Dataetisk Råds opfattelse at kravet til meningsfuld menneskelig kontrol i form af for eksempel "reel stillingtagen" bør fremgå af definitionen i § 2, stk.4. Det er også rådet opfattelse, at det vil være gavnligt for myndighederne, at loven præciserer beslutningsstøtte, snarere end at den enkelte myndighed selvstændigt skal fortolke, hvornår der er tale om beslutningsstøtte, eller afvente fremtidig afklaring i forbindelse med udvikling i retspraksis. Det er i den forbindelse rådets opfattelse, at den manglende præcision i definitionen medfører en unødvendig og uhensigtsmæssig risiko for, at myndigheder udvikler og anvender AI på en måde, som ret beset ikke kan betragtes som beslutningsstøtte, men snarere som en fuldt automatiseret beslutning.

Dataetisk Råd anbefaler derfor i lyset af det dataetiske princip om ansvarlighed, for så vidt Regeringen og Folketinget ønsker at give myndigheder en bred og almen hjemmel, at lovforslaget præciserer begrebet "beslutningsstøtte", og at denne præcisering tager udgangspunkt i, at beslutningsstøtte er anvendelse af AI der genererer en vurdering, som indgår i eller udgør grundlaget for en beslutning, men hvor en menneskelig beslutningstager har meningsfuld kontrol med beslutningen i form af kompetence til, ansvar for og ressourcer til at træffe den endelige beslutning.

2.3. Eksplicit afgrænsning af hjemmel til fuldt automatiserede beslutninger (§ 3)

Forslaget giver myndigheder hjemmel til at "udvikle og anvende AI-systemer, herunder gøre brug af beslutningsstøtte, til blandt andet evaluering af bestemte personlige forhold vedrørende en borger (profilering)…" Forslaget giver således en bred hjemmel, som eksplicit inkluderer AI til beslutningsstøtte og såkaldt profilering. Forslaget afgrænser i bemærkningerne denne brede hjemmel således, at hjemlen ikke omfatter AI til fuldt automatiserede beslutninger.

Dataetisk Råd støtter, for så vidt Regering og Folketing indfører en generel og almen hjemmel til udvikling og anvendelse af AI, at denne hjemmel begrænses til beslutningsstøtte, idet de dataetiske risici ofte er væsentligt højere ved fuldt automatiserede beslutninger end ved beslutningsstøtte.

Det er imidlertid rådets opfattelse, at en sådan afgrænsning bør fremgå klart af lovteksten således at hjemlen i § 3 ikke alene eksplicit inkluderer beslutningsstøtte og profilering, men eksplicit ekskluderer fuldt automatiserede beslutninger.

2.4. Indførelse af generelle minimumskrav for beskyttelse af følsomme persondata (§ 3, stk.2)

Forslaget giver resortministre mulighed for at fastsætte specifikke foranstaltninger på deres respektive områder for behandling af særligt følsomme personoplysninger. Forslaget fremfører i bemærkningerne, at en generel vurdering ikke vil "kunne rumme samme detaljegrad og præciseringsniveau, som vurderingen ville kunne, når foranstaltninger fastsættes ved bekendtgørelse i de relevante sektorer."

Dataetisk Råd bemærker at denne fordel må opvejes mod de mulige ulemper, herunder den øgede kompleksitet for myndigheder, som refererer til eller trækker på persondata der henhører under flere forskellige resortministerier, når ministerier anvender uensartede standarder.

Dataetisk Råd anbefaler derfor i lyset af det dataetiske princip om privatliv, for så vidt Regeringen og Folketinget ønsker at give myndigheder en bred og almen hjemmel, at loven indfører eller præciserer generelle minimumskrav for beskyttelse af særlig følsomme personoplysninger ved udvikling og anvendelse af AI med hjemmel i loven, som skal gælde på tværs af resortministerier. Dataetisk Råd anbefaler i den forbindelse, at bestemmelsen præciseres således, at resortministre alene gives mulighed for at indføre foranstaltninger som hvor nødvendigt *øger* beskyttelsen af borgeres følsomme persondata relativt til disse generelle krav.

2.5. Begrænsning af undtagelser til registreredes rettigheder (§ 4, stk.1)

Forslaget bemyndiger resortministrene til at fastsætte regler om undtagelser til registreredes rettigheder på deres respektive områder. Motivationen for denne bestemmelse anføres i bemærkningerne til loven at være, at det kan være "vanskeligt, eller i visse tilfælde sågar umuligt, for myndighederne at håndtere de registreredes rettigheder, når først personoplysningerne er indlejret i et AI-system", idet "AI-systemer [ofte er] kendetegnet ved komplekse datastrukturer, hvor oplysninger fra mange registrerede potentielt vil indgå i træningsdata, der ikke nødvendigvis tillader adskillelse af de individuelle data."

Bemærkningerne til lovforslaget påpeger muligheden for at lave generelle undtagelser, men konkluderer at "ressortministrene bør have fleksibilitet til selv at vurdere, i hvilket omfang en undtagelse eller begrænsning til den registreredes rettigheder skal gælde, herunder om begrænsningen skal gælde for hele sektorer eller for særskilte AI-systemer." Derimod berører bemærkningerne i begrænset omfang muligheden for at indføre generelle *begrænsninger* i resortministrenes muligheder for at indføre undtagelser til registreredes rettigheder, idet forslaget alene bemærker, at "…den registreredes rettigheder kun bør begrænses i det omfang, hvor det er nødvendigt."

Det er Dataetisk Råds opfattelse, at forslaget i sin eksisterende form i utilstrækkelig grad tager dataetisk hensyn til beskyttelsen af den registreredes databeskyttelsesrettigheder, idet ansvaret for dette overlades helt og holdent til de enkelte resortministre. Rådet har forståelse for, at det kan være teknisk vanskeligt at sikre eksempelvis retten til indsigt og sletning, når en borgers personlige data er blevet anvendt til udvikling af et AI-system. Det er imidlertid rådets opfattelse, at det i sådanne tilfælde må bero på en konkret og individuel vurdering, om den fordel borgere og myndigheder opnår ved at udvikle og anvende systemet, er proportionel til den indskrænkning af borgeres databeskyttelsesrettigheder, som en undtagelse fra eksempelvis retten til indsigt og sletning vil udgøre. Det er således principielt altid en mulighed, at et

ministerium snarere end at introducere en undtagelse til registreredes rettigheder, bør undlade at tillade udvikling og anvendelse af et AI-system.

Dataetisk Råd anbefaler derfor i lyset af dataetiske principper om privatliv og retssikkerhed, for så vidt Regeringen og Folketinget ønsker at give myndigheder en bred og almen hjemmel, i) at det i selve lovteksten præciseres, at resortministrenes undtagelser til registreredes rettigheder skal være nødvendige og proportionale, ii) at lovteksten præciserer hvilken karakter sådanne undtagelser kan have, herunder hvilke situationer eller hensyn som kan berettige en undtagelse, og hvilken form og detaljegrad undtagelser skal udformes i, samt iii) at lovteksten præciserer de rettigheder og situationer, hvor resortministre *ikke* har mulighed for at indføre undtagelser. Dataetisk Råd har udarbejdet en introduktion til det dataetiske hensyn om privatliv, som kan informere overvejelserne af dette arbejde.[3]

2.6. Etablering af retningslinjer for kvalitetssikring

Udvikling og anvendelse af AI til blandt andet beslutningsstøtte rejser en række udfordringer, som er veldokumenterede og -analyserede i faglitteraturen. Det drejer sig bl.a. om risiko for fejl, algoritmisk bias og uigennemsigtighed.

Risikoen for fejl drejer sig om, at AI-systemer i praksis ikke kan foretage fejlfri vurderinger. Det betyder at en myndighed, som udvikler og ønsker at anvende AI, herunder til til beslutningsstøtte, må i) teste systemet for at vurdere, hvilke typer fejl systemet kan begå og hvad fejlraten er for forskellige fejltyper, ii) finde måder at forebygge og håndtere fejl, og iii) tage stilling til det dataetiske spørgsmål om, hvor høj fejlraten må være for, at systemet kan sættes i drift.

Risikoen for algoritmisk bias drejer sig om, at AI-systemer kan have tendens til at fungere forskelligt for relevante demografiske grupper, eksempelvis således at systemet laver flere fejl for visse grupper, eller forskellige typer fejl for forskellige grupper.[4] For at håndtere udfordringen med algoritmisk bias må den offentlige myndighed i) definere de bias, som i den konkrete sammenhæng er relevante, ii) teste systemet for de pågældende bias, iii) foretage eventuel mitigering af bias, og herunder afveje modstridende hensyn til for eksempel øgede omkostninger eller tab af overordnet præcision, og iv) tage stilling til det dataetiske spørgsmål om, hvad en acceptabel tærskel er for systemets bias, før det kan sættes i drift.

Uigennemsigtighed drejer sig om, at komplekse AI-systemer kan være teknisk uigennemskuelige, i den forstand at det er vanskeligt eller umuligt selv for eksperter, i detaljer at

---

[3] https://www.dataetiskraad.dk/media/trteeyl3/dataetik-og-privatliv.pdf

[4] Se Dataetisk Råds techsplainer om algoritmisk bias: https://www.dataetiskraad.dk/media/x35nguw5/hvad-er-algoritmisk-bias_techsplainer-final-a.pdf

forstå hvordan systemet generer et output på baggrund af et input. Udfordringen behandles i lovforslaget alene i tilknytning til reglen om undtagelser fra retten til indsigt, men det er værd at bemærke, at den også vil gøre sig gældende ift. myndigheders medarbejdere, og deres mulighed for at forstå hvordan et AI-system fungerer, herunder hvilke risici systemet medfører, muligheden for at identificere fejl, og evnen til at vurdere hvilket grundlag en vurdering er truffet på, og hvor pålidelig den pågældende vurdering er. For at håndtere udfordringen med uigennemsigtighed må en offentlig myndighed i) bestemme hvilke typer indsigt det er relevant at have eller opnå for det konkrete system, ii) teste systemet for at vurdere i hvilken udstrækning det er uigennemsigtigt med hensyn til de relevante forhold, iii) om nødvendigt indføre metoder til at forklare systemet, og iv) tage stilling til det dataetiske spørgsmål om, hvorvidt systemet er tilstrækkeligt gennemsigtigt til, at det bør sættes i drift.

En central udfordring for udvikling og anvendelse af AI til beslutningsstøtte ved offentlige myndigheder er, at der både i dansk sammenhæng og internationalt i begrænset omfang er etableret retningslinjer, metoder og praksisser for at håndtere risiko for fejl, algoritmisk bias og uigennemsigtighed. I mangel af etablerede retningslinjer, metoder og praksisser, overlades ansvaret til den enkelte myndighed. Forslaget berører i begrænset omfang risiko for fejl og uigennemsigtighed, og anfører om algoritmisk bias i bemærkningerne blot at "[m]yndighederne skal derfor bl.a. selv konkret vurdere med afsæt i de relevante regelsæt, hvilke mitigerende foranstaltninger, som vil være relevante at implementere for at begrænse eventuel påvirkning fra bias i AI-systemet i forbindelse med beslutningsstøtte…" Det forekommer i bedste fald at være en ressourcekrævende opgave, at overlade ansvaret for at håndtere disse udfordringer til hver enkelt myndighed, som i givet fald sideløbende vil skulle tage stilling til de samme udfordringer og løsninger. I praksis er det Dataetisk Råds vurdering at denne uddelegering af ansvaret medfører en betragtelig risiko for, at myndigheder ikke i tilstrækkelig grad vil håndtere udfordringerne. Det er således Dataetisk Råds opfattelse, at det er dataetisk stærkt betænkeligt, at give offentlige myndigheder en bred og almen hjemmel til udvikling og anvendelse af AI til beslutningsstøtte i fraværet af retningslinjer, som kan støtte dataetisk kvalitetssikring af de pågældende systemer.

Dataetisk Råd anbefaler derfor i lyset af dataetiske principper om at gøre gavn, ikke skade, sikre retfærdighed, velfærd, forklarlighed og lighed, for så vidt Regeringen og Folketinget ønsker at give myndigheder en bred og almen hjemmel, at der i tilknytning til lovforslaget udarbejdes konkrete og detaljerede retningslinjer for hvordan offentlige myndigheder, som ønsker at gøre brug af den indførte hjemmel, skal kvalitetssikre systemerne, herunder forholde sig til og håndtere risikoen for fejl, algoritmisk bias og uigennemsigtighed, inklusive klare standarder for hvilke niveauer af fejl, bias og uigennemsigtighed som er acceptable for AI-systemer, der skal sættes i drift. Dataetisk Råd har i 2025 udarbejdet en rapport om den dataetiske udfordring med

risiko for fejl ved offentlige myndigheders anvendelse af generativ AI, som kan informere overvejelser om og udvikling af sådanne retningslinjer.[5]

For så vidt de relevante retningslinjer og standarder varierer på tværs af resortministrene, kan opgaven placeres hos de enkelte ministerier, men det er Dataetisk Råds opfattelse, at det vil være både muligt og ønskeligt at etablere fælles minimumsstandarder, som resortministrene om nødvendigt kan afvige fra, ved at implementere *højere* krav til AI-systemer i tilknytning til det enkelte ministeriums resort.

2.7. Udførelse af dataetisk konsekvensanalyse

En dataetisk konsekvensanalyse belyser de dataetiske konsekvenser af en given digital teknologi, en ny praksis for anvendelse af en teknologi, eller en ændring i reglerne for udvikling og anvendelse af teknologien. Formålet med en dataetisk konsekvensanalyse er at give et præcist og detaljeret overblik over hvilke etiske hensyn, som berøres af den evaluerede teknologi, praksis eller regelændring. Derved bliver det muligt både at overveje mitigerende foranstaltninger, som kan afbøde evt. risici eller ulemper, og at tage samlet stilling til, om teknologien, praksissen eller regelændringen er dataetisk forsvarlig.

Det nærværende lovforslag indfører en bred hjemmel til udvikling og anvendelse af AI til beslutningsstøtte ved offentlige myndigheder, samt anvendelse af persondata til disse formål. Forslaget berører således både personers privatliv, og deres møde med offentlige myndigheder, som kan træffe beslutninger af væsentlig og i nogle tilfælde afgørende betydning for den enkelte borgers liv og velfærd.

Dataetisk Råd anbefaler derfor, for så vidt Regeringen og Folketinget ønsker at give myndigheder en bred og almen hjemmel, at Digitaliseringsstyrelsen udarbejder en dataetisk konsekvensanalyse, der grundigt belyser de etiske hensyn som er på spil, og implikationerne af den foreslåede lov. Dataetisk Råd har udarbejdet en guide til dataetisk metode, som kan informere en sådan dataetisk konsekvensanalyse.[6]

2.8. Bred hjemmel – fordele og ulemper (§ 3, stk.1)

Forslaget giver offentlige myndigheder en bred og almen hjemmel til udvikling og anvendelse af AI ved offentlige myndigheder, inklusiv til beslutningsstøtte. En sådan hjemmel vil gøre det muligt for offentlige myndigheder at anvende persondata til udvikling og anvendelse af AI til beslutningsstøtte. Derved får samtlige offentlige myndigheder mulighed for umiddelbart at gå i gang med at udvikle og anvende teknologien.

---

[5] https://www.dataetiskraad.dk/media/t3mi1akn/dataetisk-raads-rapport-om-generativ-ai.pdf
[6] https://www.dataetiskraad.dk/udgivelser/dataetik-saadan-goer-du

Alternativet til en bred og almen hjemmel er enten status quo, hvor offentlige myndigheder i vid udstrækning savner lovhjemmel til brug af persondata til udvikling og anvendelse af AI til beslutningsstøtte, eller at Regering og Folketing giver specifikke hjemler til individuelle myndigheders udvikling og anvendelse af konkrete AI-systemer, således som det allerede er tilfældet for en række myndigheder. Ulempen ved det første alternativ er, at den offentlige sektor går glip af de fordele, som udvikling og anvendelse af AI kan medføre. Ulempen ved det andet alternativ er, at myndigheder, som ønsker at udvikle og anvende AI, må afvente at de gives individuel hjemmel, samt at Regering og/eller Folketing pålægges at tage stilling til og udstede hjemmel i hvert enkelt tilfælde.

Ikke desto mindre er det Dataetisk Råds opfattelse, at det i den forhåndenværende situation er værd at overveje, om det er hensigtsmæssigt at udstede en bred og almen hjemmel, snarere end at give individuelle myndigheder specifik hjemmel til konkrete udviklinger og anvendelser. Det er rådets vurdering, at der fortsat er både begrænsede retningslinjer for og erfaringer med hvordan offentlige myndigheder etisk kan udvikle og anvende AI til beslutningsstøtte, samt at en bred og almen hjemmel, i modsætning til specifikke hjemler målrettet den individuelle myndighed og/eller den konkrete anvendelse, vil gøre det vanskeligt, at vurdere risici og nødvendige forholdsregler. Ved at lovfæste en bred og almen hjemmel mister Regering og Folketing således muligheden for i de enkelte tilfælde at tage stilling til, om der bør udstedes hjemmel til den konkrete anvendelse, herunder muligheden for at indhente høringssvar, som kan belyse fordele og ulemper, samt at indføre målrettede rammer og betingelser for den konkrete anvendelse.

Dataetisk Råd anbefaler i lyset af disse overvejelser, af Regering og Folketing overvejer, om det er hensigtsmæssigt at give offentlige myndigheder en bred og almen hjemmel, snarere end løbende at udstede specifik hjemmel til individuelle myndigheder, hvor udvikling og anvendelse af AI vurderes at være dataetisk forsvarlig.

3. Afsluttende bemærkninger

AI er en banebrydende ny teknologi, som har potentiale til på afgørende vis at ændre den danske offentlige sektor til gavn for både myndigheder og borgere. Alle nye teknologier rejser etiske udfordringer, som vi som samfund skal finde måder at håndtere, for at realisere gevinsterne uden at realisere risici. For velkendte teknologier har vi udviklet systemer og institutioner til at definere standarder og kvalitetssikre produkter. Udvikling og anvendelse af lægemidler i Danmark foregår i en velreguleret institutionel ramme der garanterer, at nye lægemidler er sikre og virkningsfulde. For nye digitale teknologier som AI er vi stadig som samfund i færd med at skabe de rammer, som skal sikre, at vi udvikler og anvender teknologierne etisk. Det er vigtigt at vores udvikling af disse rammer går hånd i hånd med den

teknologiske udvikling, så teknologien hverken sinkes af eller løber fra vores forståelse af, hvordan vi kan bruge den sikkert og gavnligt.

Rådet står til rådighed for dialog og faglig sparring i den videre proces og bidrager gerne med viden og værktøjer til at støtte den etiske udvikling og anvendelse af AI til beslutningsstøtte ved offentlige myndigheder.

Med venlig hilsen på vegne af Dataetisk Råd,

Johan Busse



Formand

Dataetisk Råd

DATATILSYNET

Digitaliseringsstyrelsen
Landgreven 4
1301 København K
Sendt til: jonmei@digst.dk, emimol@digst.dk, lea-omd@digst.dk og kahevi@digst.dk
Kopi sendt til: jm@jm.dk

9. oktober 2026

J.nr. 2026-11-0591
Dok.nr. 935516
Sagsbehandler
Signe Vestergård Spring

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Høring over udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

1. Indledning

Digitaliseringsstyrelsen har den 14. september 2026 anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast til lovforslag.

Datatilsynet har den 3. marts 2026 fremsendt bemærkninger til det tidligere fremsendte udkast til lovforslag (udkast til forslag til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning). Datatilsynets høringssvar vedlægges.

Digitaliseringsstyrelsen har oplyst, at styrelsen har modtaget en række høringssvar til det tidligere udkast til lovforslag, og at styrelsen på den baggrund har foretaget en række ændringer i udkastet.

Datatilsynet skal i forbindelse med det ovennævnte nye udkast til lovforslag udtale følgende, som skal ses i sammenhæng med det tidligere fremsendte høringssvar:

2. Generelle bemærkninger

2.1. Det fremgår af afsnit 1.1. i udkastets almindelige bemærkninger, at formålet er at skabe en generel databeskyttelsesretlig hjemmel, der samtidig giver et tydeligere retsgrundlag for offentlige myndigheders og organers mulighed for at udvikle og anvende AI-systemer ved behandling af personoplysninger efter databeskyttelsesforordningen for at understøtte myndighedernes og organernes opgavevaretagelse efter anden lovgivning.

Herefter fremgår det, at en generel databeskyttelsesretlig hjemmel vil indebære, at offentlige myndigheder og organer – som led i myndighedens eller organets allerede fastlagte og afgrænsede opgavevaretagelse – vil kunne beslutte at behandle personoplysninger efter databeskyttelsesforordningen ved brug af kunstig intelligens i form af et AI-system til bl.a. beslutningsstøtte, herunder ved evaluering af bestemte personlige forhold vedrørende en borger, uden først at skulle etablere nye selvstændige databeskyttelsesretlige hjemler i sektorlovgivningen.

Som i det tidligere udkast fremgår det derudover, at lovforslaget helt overordnet vil gøre det muligt for offentlige myndigheder og organer at anvende AI-systemer i deres opgavevareta-

gelse på samme måde, som myndigheder og organer i dag anvender andre elektroniske hjælpemidler i deres opgavevaretagelse m.v.

Datatilsynet har med tilfredshed noteret sig, at det i det nye udkast er tilføjet, at etableringen af et supplerende databeskyttelsesretligt retsgrundlag til at behandle personoplysninger ved brug af AI-systemer ikke i sig selv sikrer, at de behandlingsaktiviteter, som foretages i forbindelse hermed, sker fuldt ud lovligt. I den forbindelse fremgår det, at den dataansvarlige, f.eks. myndigheden eller organet, inden behandlingen påbegyndes og igennem hele AI-systemets livscyklus skal sikre, at reglerne i databeskyttelsesforordningen, databeskyttelsesloven og anden for behandlingerne relevant lovgivning kan overholdes.

Af databeskyttelsesforordningens artikel 25, stk. 1, fremgår, at en dataansvarlig allerede på tidspunktet for fastlæggelsen af midlerne til behandlingen og på tidspunktet for selve behandlingen, implementerer passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på effektiv implementering af de grundlæggende principper. Derudover skal foranstaltningerne være designet med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i databeskyttelsesforordningen og beskyttelse af de registreredes rettigheder. I vurderingen af hvilke foranstaltninger der skal gennemføres, skal flere forhold, der er nævnt i bestemmelsen, tages i betragtning.

Det medfører efter Datatilsynet opfattelse, at det allerede ved designet eller valget af en given løsning til behandlingen af personoplysninger skal vurderes om løsningen – i sit design – rent faktisk kan levere den fornødne overholdelse af forordningen. Dette er særligt væsentligt, hvor den dataansvarlige har konstateret, at behandlingen i sig selv sandsynligvis vil indebære en høj risiko for de registreredes rettigheder. Hvis det sidstnævnte gør sig gældende, vil denne type af behandlinger ofte kræve en betydelig grad af tekniske foranstaltninger – i løsningens design – for effektivt at kunne nedsætte den iboende risiko på tidspunktet, hvor selve behandlingen iværksættes.

Ovennævnte indebærer, at hvis det – ved et givet design – er vurderingen, at behandlingens karakter, omfang, sammenhæng og formål samt risiciene for de registreredes rettigheder indebærer, at den beskyttelse, som forordningen giver de registrerede, undermineres, skal dette føre til gentænkning af det valgte design.

Det er Datatilsynets erfaring, at flere AI-produkter leveres som standardiserede ydelser, hvor den enkelte organisation som kunde som regel har begrænsede muligheder for at tilpasse den pågældende service til organisationens individuelle behov og krav, herunder kravene efter databeskyttelsesreglerne. Disse problemstillinger er ikke nye, men er forhold som Datatilsynet tidligere har vejledt om i relation til anden servicebaseret arkitektur, f.eks. i tilsynets cloudvejledning.[1] Det er dermed vigtigt, at de dataansvarlige forud for indkøb af et AI-produkt undersøger, om det er muligt at foretage de ændringer i såvel kontraktsgrundlaget som funktionaliteten, der er nødvendige, for at løsningen kan benyttes til behandling af personoplysninger i overensstemmelse med databeskyttelsesreglerne.

Datatilsynet opfordrer på den baggrund til, at det indarbejdes i den dataansvarliges indkøbs- og projektmodel for forretningsudvikling og teknologisk understøttelse, at der både tidsmæssigt og økonomisk afsættes råderum til, at der kan afsøges sådanne andre design eller andre løsninger, der i sit design nedsætter de identificerede risici.

1 Der henvises til Datatilsynets vejledning om cloud (marts 2022)

2.2. I lovudkastet er de økonomiske konsekvenser og implementeringskonsekvenserne for det offentlige beskrevet.

Det følgende fremgår i den forbindelse af afsnit 5 i udkastets almindelige bemærkninger:

> ”Ved at give offentlige myndigheder og organer hjemmel til at udvikle og anvende AI-systemer, der behandler personoplysninger, som led i deres opgavevaretagelse efter anden lovgivning, vurderes det, at myndighederne og organerne kan opnå effektiviseringsgevinster og frigive tid til kerneopgaven. Dette beror på, at AI-systemer vil kunne frigive tid ved særligt at understøtte områder med hyppige og ensartede sager og processer. Dette kunne f.eks. være tjek og indsamling af dokumentation i sagsbehandlingen, udarbejdelse af referater eller lignende. Samtidig vil en generel databeskyttelsesretlig hjemmel, som tilvejebringes i dette lovforslag medføre, at offentlige myndigheder og organer i mindre grad forventes at have behov for at indkøbe ekstern bistand for at afklare rammerne for, hvornår og i hvilket omfang de må udvikle og anvende AI-systemer i deres opgavevaretagelse.”

Endvidere fremgår det, at omkostningerne forbundet med udvikling og anvendelse af AI-systemer kan tage form af implementeringsomkostninger forbundet med eventuelt indkøb, træning og implementering af AI-systemer i drift. Det fremgår herudover, at der kan være omkostninger relateret til oplæring af medarbejdere og løbende vedligehold af AI-systemer. Forsknings-, Uddannelses- og Digitaliseringsministeriet vurderer, at disse omkostninger vil være højest i begyndelsen af implementeringsprocessen, hvorefter de vil blive opvejet af gevinsterne ved anvendelsen af AI-systemer i myndighedernes og organernes opgavevaretagelse.

Datatilsynet ser gerne, at det nuanceres i udkastets bemærkninger, at der udover de ressourcebetragtninger, Forsknings-, Uddannelses- og Digitaliseringsministeriets henviser til, skal påregnes et ikke ubetydeligt arbejde med at sikre beskyttelse af borgernes personoplysninger som følge af mange AI-systemers funktionsmåde. Denne indsats må forventes at være af mere kontinuerlig karakter, end udkastet giver udtryk for. En af de væsentlige grunde er, at AI-ydelserne er i hastig udvikling, og såvel funktionalitet og måden en given ydelse leveres på som kontraktsgrundlaget herfor er undergivet hyppige ændringer.

Datatilsynet bemærker i den forbindelse, at der ved indkøb af AI-systemer bør være en særlig opmærksomhed på den grundmodel, dvs. det standardprodukt fra en leverandør, som AI-systemet er baseret på. Det gælder også, hvis hensigten er, at systemet skal videreudvikles ved brug af personoplysninger om borgerne.

Det skyldes, at AI-systemer ofte er karakteriseret ved betydelig kompleksitet og manglende gennemsigtighed. Det kan derfor være særdeles vanskeligt for de dataansvarlige at få en tilstrækkelig forståelse af AI-systemets opbygning og de behandlinger, der foretages, som er en forudsætning for at kunne sikre beskyttelse af borgernes personoplysninger i overensstemmelse med databeskyttelsesreglerne.

Derudover vil der for nogle indkøbte AI-systemer ofte ske ændringer i aftalegrundlaget med leverandørerne, der regulerer AI-systemets funktioner samt leverandørers og underleverandørers behandling af personoplysninger. Der må som følge af de ofte uklare behandlingskonstruktioner derfor påregnes et ikke ubetydeligt ressourceforbrug hos myndigheder og organer med løbende at danne et tilstrækkeligt overblik over den behandling af personoplysninger, der foregår i forbindelse med anvendelse og eventuelt (videre)udvikling af AI-systemet, herunder ved leverandørers og underleverandørers behandling af personoplysninger.

Den dataansvarlige skal have adgang til de nødvendige ressourcer til at sikre lovlig behandling af personoplysninger. Det gælder også i situationer, hvor et valgt produkt eller aftalegrundlaget for produktet ændrer sig.[2]

For mange offentlige myndigheder og organer vil det derfor være nødvendigt at bruge betydelige ressourcer, herunder på f.eks. ekstern bistand, i forbindelse med indkøb og implementering af AI-systemer – men også når systemet anvendes i drift og i løbet af hele AI-systemets livscyklus.

Datatilsynet bemærker i den forbindelse, at hvis dette arbejde ikke foretages, inden behandlingsaktiviteterne påbegyndes, vil der ofte være store omkostninger forbundet med efterfølgende at håndtere de eventuelle negative afledte konsekvenser, som AI-systemet medfører for borgerne og/eller myndigheden. Dette vil bl.a. være tilfældet, hvis brugen af et sådant AI-system indebærer, at myndigheden træffer forkerte afgørelser eller foretager forkerte tiltag i forbindelse med myndighedens opgavevaretagelse.

2.3. Med henvisning til afsnit 4.4. i Datatilsynets tidligere høringssvar er det fortsat tilsynets opfattelse, at den foreslåede tilgang i udkastets § 3 rejser væsentlige spørgsmål i relation til databeskyttelse.

Det skyldes, at udkastets bestemmelser stadig fastsætter meget vide rammer for en bred kreds af myndigheder og virksomheder m.v. til at behandle personoplysninger om et stort antal registrerede, herunder sårbare borgere. Disse behandlingsaktiviteter kan i nogle sammenhænge medføre høje risici for de registreredes rettigheder og frihedsrettigheder, som følge af den måde AI-systemers behandlingsaktiviteter og resultatgenerering sker på.

Det er på den baggrund stadig Datatilsynets opfattelse, at en så vid adgang i bestemmelsen til at behandle personoplysninger, der potentielt kan være meget indgribende for de registrerede, kan øge risikoen for konkrete og ikke-proportionelle indgreb i privatlivets fred.

Endvidere finder Datatilsynet, at det fortsat vil være nødvendigt for myndighederne at foretage en vurdering af den eksisterende sektorlovgivning i forhold til, om det fremgår klart, at myndighedens opgavevaretagelse indebærer den pågældende behandling af personoplysninger, herunder i forbindelse med, at der træffes afgørelser eller iværksættes tiltag.

Det er herudover fortsat ikke indlysende for Datatilsynet, at den foreslåede ordning i udkastet lever op til kravene i artikel 23. Det gælder både i forhold til muligheden for at behandle personoplysninger fra myndighedernes historiske og lukkede sager til udvikling af AI-systemer uden at foretage en vurdering efter databeskyttelsesforordningens artikel 6, stk. 4, samt i forhold til ressortministrenes mulighed for at fastsætte regler, der helt eller delvist begrænser de registreredes rettigheder efter artikel 12 og artikel 15-21 i databeskyttelsesforordningen.

3. Anvendelsesområde

Udkastets § 1 vedrører lovens anvendelsesområde. Det fremgår af udkastets § 1, at loven gælder for alle offentlige myndigheder og organer, i det omfang disse behandler personoplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e til opgaver, der udføres i samfundets interesse eller, som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

2 Der henvises til Datatilsynets afgørelser i sagen med j.nr. 2025-431-0053 (den såkaldte Chromebook-sag).

Det fremgår af udkastets bemærkninger til bestemmelsen, at den foreslåede ordning vil indebære, at samtlige relevante aktører, der vil skulle varetage opgaver i samfundets interesse og myndighedsopgaver, og dermed foretager behandling af personoplysninger med hjemmel i artikel 6, stk. 1, litra e, i databeskyttelsesforordningen, vil få mulighed for at behandle personoplysninger ved udvikling og anvendelse af AI-systemer.

Endvidere fremgår det, at "offentlige myndigheder" og "organer" skal forstås bredt, hvorfor anvendelsesområdet omfatter myndigheder og organer, der er omfattet af lignende begreber i anden relevant lovgivning, og det omfatter alle relevante dele af f.eks. den offentlige forvaltning, som varetager myndighedsopgaver og forvaltningsopgaver. Der er i den forbindelse henvist til forvaltningslovens § 1, stk. 1-3 og udbudslovens § 24, nr. 27, men Forsknings-, Uddannelses- og Digitaliseringsministeriets understreger i den forbindelse, at anvendelsesområdet ikke er afgrænset til myndigheder og organer som defineret i henholdsvis forvaltningsloven og udbudsloven, og at andre myndigheder og organer ligeledes vil være omfattet af lovforslaget.

For så vidt angår private aktører fremgår det, at disse aktører, der kun delvist udfører opgaver i samfundets interesse eller myndighedsopgaver, alene vil kunne anvende det supplerende retsgrundlag i det omfang, at deres behandling af personoplysninger sker med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e.

I udkastet nævnes eksempler på offentlige myndigheder og organer, som omfattes af reglerne. I den forbindelse er det i forhold til det tidligere fremsendte udkast tilføjet, at lovforslaget også vil omfatte organer som varetager myndighedsopgaver – som f.eks. kommunalt ejede forsyningsselskaber.

Det står ikke Datatilsynet klart, hvor mange private aktører og på hvilke områder af disse private aktørers behandlingsaktiviteter, loven kommer til at finde anvendelse for. Det foreslåede anvendelsesområde i udkastets § 1 må forventes at give anledning til en række afgrænsningsproblemer. Datatilsynet skal herudover pege på, at udkastets § 3 efter tilsynets opfattelse ikke vil kunne udgøre en hjemmel til videregivelse af personoplysninger til private aktørers brug af oplysningerne til egne formål.

Det følgende fremgår af afsnit 2.1.2. i udkastets almindelige bemærkninger:

> "Det er Forsknings-, Uddannelses- og Digitaliseringsministeriets vurdering, at anvendelsesområdet for den foreslåede ordning vil skulle afgrænses på baggrund af offentlige myndigheders og organers konkrete behandlingsaktiviteter, således at lovforslaget omfatter behandlingsaktiviteter, der foretages med hjemmel i artikel 6, stk. 1, litra e, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen) med senere ændringer, dvs. når behandlingen udføres i samfundets interesse eller, når behandlingen henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt."

Derudover fremgår det følgende af afsnittet:

> "Den foreslåede ordning vil således finde anvendelse sideløbende med anden sektorlovgivning, uden at dette vil påvirke lovens anvendelsesområde eller den fortsatte anvendelse af den pågældende sektorlovgivning.
>
> Det bemærkes, at det i forbindelse med en eventuel fremtidig revision af sektorlovgivning, som regulerer det samme anvendelsesområde, kan være relevant for ressortministrene at overveje, om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i stedet bør ske med hjemmel i dette lovforslag. Det kan f.eks. være relevant i tilfælde, hvor den foreslåede ordning i dette lovforslag vil sikre et højere beskyttelsesniveau for den registreredes rettigheder og interesser, og indebære en højere grad af detaljeringsniveau og dermed øget transparens, eller hvor

> hensynet til ensartethed i lovgivningen i øvrigt taler herfor. Ved vurderingen af den eksisterende sektorlovgivnings egnethed bør der lægges vægt på, hvilke områder og behandlingsaktiviteter AI-systemet er tiltænkt anvendt til. Hvis AI systemet f.eks. skal anvendes over for særligt sårbare grupper af registrerede, taler dette i særlig grad for at overveje, hvordan der kan sikres det højest mulige beskyttelsesniveau for de registrerede."

Det er Datatilsynets opfattelse, at det fortsat vil være nødvendigt for myndighederne og organerne at foretage en vurdering af den eksisterende sektorlovgivning i forhold til, om det fremgår, at myndigheden eller organet er forpligtet eller berettiget til at udføre den pågældende opgave, som ønskes understøttet af et AI-system. Behandlingen af personoplysninger skal – uanset hvilken teknologi der anvendes – være nødvendig for udførelsen af den pågældende opgave i samfundets interesse eller som en del af myndighedsudøvelsen. Bestemmelserne i dette udkast kan derfor ikke medføre en udvidelse af de behandlingsaktiviteter, som myndighederne og organerne i dag foretager på baggrund af den relevante sektorlovgivning, og som ønskes understøttet af AI.

Derudover bemærker Datatilsynet, at udkastet efter tilsynets opfattelse ikke indebærer en høj grad af detaljeringsniveau og transparens for borgerne, som følge af det brede anvendelsesområde, bestemmelserne skal finde anvendelse på.

Datatilsynet har endvidere noteret sig, at det fremgår af det afsnit 2.1.1.1 i udkastets almindelige bemærkninger, at den foreslåede ordning alene vil finde anvendelse på behandling af personoplysninger, der er omfattet af databeskyttelsesforordningen, og at udkastet ikke finder anvendelse på behandling af personoplysninger, der er reguleret af f.eks. retshåndhævelsesloven. Datatilsynet lægger på den baggrund til grund, at reglerne i udkastet heller ikke skal finde anvendelse for politiets og forsvarets efterretningstjenesters behandling af personoplysninger.

4. Definitioner

4.1. "Beslutningstøtte" defineres i udkastets § 2, nr. 4, som: "Enhver form for forslag eller anbefaling til afgørelser eller væsentlige tiltag overfor den registrerede, som er genereret af et AI system, og som en fysisk person inddrager i den samlede faglige vurdering, som ligger til grund for afgørelsen eller tiltaget, uden at AI-systemet selv træffer afgørelsen eller iværksætter tiltaget."

Datatilsynet lægger til grund, at det er den dataansvarlige myndighed eller organ, der inddrager et forslag eller anbefalinger til afgørelser eller væsentlige tiltag over for den registrerede i sin samlede faglige vurdering, og at "en fysisk person" er en medarbejder eller en anden person tilknyttet den dataansvarlige myndighed eller organ.

I det nye udkast er kravet til menneskelig indgriben uddybet i forhold til, hvornår der er tale om beslutningsstøtte og ikke automatiske afgørelser eller tiltag. Det fremgår i den forbindelse af afsnit 2.1.2. i udkastets almindelige bemærkninger, at menneskelig involvering i så ringe en grad, at det alene anses som en formalitet, ikke vil kunne anses som beslutningsstøtte, da AI-systemet reelt foretager beslutningen. Derudover fremgår det, at der vil være en forventning om, at menneskelig involvering skal omfatte en reel stillingtagen til eller vurdering af AI-systemets anbefalinger og forslag, førend der er tale om beslutningsstøtte.

Der er i den forbindelse tilføjet eksempler på foranstaltninger, der skal sikre og dokumentere, at den menneskelige involvering er reel og ikke alene udgør en formalitet. Her fremgår det følgende: "Identificering af hvem der har beslutningskompetencen ved brug af AI-systemet, fastlæggelse af hvordan afvigelser fra AI-systemets anbefalinger og forslag håndteres og dokumenteres og logning af anvendelsen af AI-systemet". Det fremgår herefter, at det afgørende

fortsat er, om den person, der har beslutningskompetencen foretager en reel og selvstændig vurdering af AI-systemets anbefaling eller forslag.

Datatilsynet bemærker i den forbindelse, at for at sikre reel menneskelig involvering og et meningsfuldt tilsyn med afgørelsen, skal de personer, der reelt skal træffe afgørelsen – og som har den fornødne kompetence – sættes i stand til at evaluere de faktuelle omstændigheder, som beslutningen træffes på baggrund af. Dette er nødvendigt for at verificere, at det nødvendige og retvisende faktum inddrages i sagens afgørelse. Dette kan imidlertid i forhold til nogle AI-systemer være vanskeligt på grund af AI-systemets kompleksitet og manglende gennemsigtighed.

Det kan endvidere være særdeles vanskeligt for de dataansvarlige at kvalitetssikre disse systemer, så det sikres, at de output, AI-systemet giver – f.eks. forslag eller anbefalinger til afgørelser eller tiltag over for borgerne – er korrekte og ikke er urimelige. De dataansvarlige myndigheder er forpligtede til at identificere og håndtere eventuel bias i det output, AI-systemet giver. Bias kan f.eks. skyldes kvaliteten af de data, som grundmodellen er trænet på, og det kan føre til diskrimination eller urimelig behandling af en borger eller grupper af borgere.

Derudover er det vigtigt, at de dataansvarlige myndigheder og organer er opmærksomme på risikoen for "automation bias", hvor f.eks. sagsbehandlere tillægger systemets vurdering af en sag større betydning end deres egen vurdering. I så fald vil systemet de facto afgøre sagen, og der vil være tale om en automatisk afgørelse.

Begrebet "fuldautomatiske afgørelser" er nævnt flere steder i udkastet. Datatilsynet bemærker, at retten i databeskyttelsesforordningens artikel 22 til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling eller profilering, ikke er begrænset til fuldautomatiske afgørelser.

4.2. "Udvikling" defineres i udkastets § 2, nr. 5, som: "Enhver aktivitet der bidrager til udviklingen af et AI-system, herunder skabelse, træning, afprøvning og validering. Udvikling omfatter også lignende aktiviteter, der foretages efter AI-systemet er taget i brug, herunder gentræning og videreudvikling."

Det følgende fremgår af udkastets bemærkninger til bestemmelsen:

> "Begrebet vil også omfatte lignende aktiviteter, der foretages efter, AI-systemet er taget i brug i forbindelse med den enkelte myndigheds varetagelse af forskellige myndighedsopgaver, herunder gentræning og videreudvikling. Udvikling og anvendelse af et AI-system vil således typisk være en iterativ proces bestående af en række faser, der ikke nødvendigvis sker i en bestemt rækkefølge. Der vil i praksis derfor godt kunne være en mere flydende overgang mellem begrebet "udvikling" og begrebet "anvendelse", hvorfor de forskellige faser i AI-systemets livscyklus kan være svære at adskille. Det skal dog understreges, at lovforslaget både vil kunne anvendes som supplerende retsgrundlag i forbindelse med udvikling og anvendelse af et AI-system, hvorfor det ikke vil være et krav efter dette lovforslag, at myndigheden konkret kan angive, hvilken fase af AI-systemets livscyklus der er tale om for at kunne anvende lovforslaget som et supplerende retsgrundlag."

Datatilsynet bemærker i den forbindelse, at databeskyttelsesreglerne indeholder et generelt krav om, at personoplysninger kun må behandles til et udtrykkeligt angivet og legitimt formål.[3]

Udviklingen (og videreudviklingen) af et AI-system skal efter Datatilsynets opfattelses anses som et formål i sig selv i forhold til databeskyttelsesreglerne. Behandling af personoplysninger

3 Databeskyttelsesforordningens artikel 5, stk. 1, litra b

med henblik på at udvikle nye teknologiske løsninger tjener i sagens natur et andet formål end behandling af personoplysninger som led i myndighedens daglige drift. Det gælder også, selv om det langsigtede formål med at udvikle løsningen er at anvende den i myndighedens daglige drift.[4]

Det er dermed et krav efter de databeskyttelsesretlige regler, at de dataansvarlige kan angive, hvad formålet er med behandlingen af oplysninger i de forskellige faser i AI-systemets livscyklus.

De forskellige behandlingsaktiviteter og formålene med behandlingen skal også angives i konsekvensanalyser vedrørende databeskyttelse.[5] En sådan konsekvensanalyse vil efter Datatilsynets opfattelse næsten i alle tilfælde være et krav forud for behandling af personoplysninger som led i udvikling og/eller drift af AI-systemer, da disse behandlingsaktiviteter vil udløse flere af de kriterier, der er udslagsgivende for, om der skal gennemføres en konsekvensanalyse.[6]

5. Supplerende retsgrundlag

5.1. Det følger af udkastets § 3, stk. 1, at offentlige myndigheder og organer kan udvikle og anvende AI-systemer, herunder gøre brug af beslutningsstøtte, til blandt andet evaluering af bestemte personlige forhold vedrørende en borger (profilering) på baggrund af personoplysninger, som myndigheden eller organet behandler, for at understøtte myndighedens eller organets opgavevaretagelse efter anden lovgivning, jf. dog stk. 2.

Datatilsynet har forstået, at det er hensigten, at § 3, stk. 1, skal fungere som supplerende retsgrundlag for behandling af personoplysninger i forbindelse med offentlige myndigheder og organers udvikling og anvendelse af AI-systemer, der skal understøtte myndighedens eller organets opgavevaretagelse efter anden lovgivning. Det er dermed Datatilsynets forståelse, at bestemmelsen skal kunne anvendes i alle sammenhænge i den offentlige forvaltning, hvor der behandles personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, og et supplerende retsgrundlag i den pågældende sektorlovgivning.

Det fremgår af udkastets bemærkninger til § 3, stk. 1, at offentlige myndigheders og organers brug af AI-systemer til at varetage opgaver efter anden lovgivning bl.a. vil kunne omfatte beslutningsstøtte. Det fremgår i den forbindelse, at det vil betyde, at beslutningsstøtte, herunder ved evaluering af bestemte personlige forhold vedrørende en borger (profilering), vil kunne foretages, hvis det sker i forbindelse med offentlige myndigheders og organers opgavevaretagelse.

Datatilsynet bemærker i den forbindelse, at de dataansvarlige offentlige myndigheder og organer skal foretage en vurdering af, om behandlingen er *nødvendig* af hensyn til udførelsen af en opgave, som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Artikel 29-gruppen har tidligere udtalt, at den pågældende myndighedsopgave eller -funktion skal have et klart retsgrundlag, hvis artikel 6, stk. 1, litra e, skal anvendes som hjemmel til profilering.[7] Datatilsynet henviser derudover til afsnit 4.3 i sit tidligere høringssvar, hvor profilering er nærmere omtalt.

4 Der henvises til afsnit 3.1 i Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens (oktober 2023). Derudover henvises til præmis 40-43 i EU-Domstolens dom af 20. oktober 2022 i sag C-77/21, hvor Domstolen synes at forudsætte, at foretagelse af test og korrektion for fejl af et it-system udgør et separat formål fra opfyldelse af abonnementsaftaler fra kunder, som it-systemet oprindeligt understøttede.

5 Det følger af databeskyttelsesforordningens artikel 35, stk. 7, litra a.

6 Der henvises til afsnit 6 i Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens (oktober 2023).

7 Side 9 i Artikel 29-gruppens retningslinjer om automatiske individuelle afgørelser om profilering i henhold til forordning 2016/679, WP251. EDPB har ved Endorsement 1/2018 af 25. maj 2018 tilsluttet sig retningslinjerne.

5.2. Det følger af afsnit 2.2.1.1.1 i udkastets almindelige bemærkninger, at behandling af personoplysninger kun er lovlig, hvis og i det omfang mindst ét af forholdende i bestemmelsens litra a-f gør sig gældende. I den forbindelse fremgår det, at for offentlige myndigheders og organers behandling af personoplysninger er særligt databeskyttelsesforordningens artikel 6, stk. 1, litra e, relevant.

Datatilsynet bemærker i den forbindelse, at offentlige myndigheder også kan behandle personoplysninger efter artikel 6, stk. 1, litra c, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige. Der er imidlertid inden for den offentlige sektor et betydeligt overlap mellem artikel 6, stk. 1, litra c og e.

Kravene til et supplerende retsgrundlag er nærmere beskrevet i samme afsnit i udkastet. I den forbindelse er artikel 6, stk. 2 og 3 og præambelbetragtning nr. 45 gengivet. Datatilsynet ser i den forbindelse gerne, at bestemmelsernes og præambelbetragtningens ordlyd gengives. Det bør i den forbindelse tilføjes i henvisningen til præambelbetragtning nr. 45, at det kan være tilstrækkeligt med en lov som grundlag for adskillige behandlingsaktiviteter, som er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse.

Datatilsynet skal derudover henvise til tilsynets bemærkninger om kravene til et supplerende retsgrundlag i det tidligere fremsendte høringssvar.

5.3. Det følgende fremgår derudover af afsnit 2.2.1.1.1. af udkastets almindelige bemærkninger:

> ”Datatilsynet har i sin praksis ad flere omgange udtalt sig om spørgsmålet om kravene til det supplerende retsgrundlag efter databeskyttelsesforordningen i forbindelse med offentlige myndigheders og organers anvendelse af kunstig intelligens. Denne praksis har resulteret i en strengere tilgang til hjemmelskravet i de tilfælde, hvor der anvendes AI-systemer, hvilket ikke følger den almindelige tilgang om teknologineutralitet [Datatilsynets fremhævning]. Derimod ses det nu, at brugen af kunstig intelligens-løsninger, der – i de tilfælde, hvor behandlingsaktiviteten vil være indgribende overfor de registrerede – nødvendiggør et supplerende retsgrundlag, der beskriver brugen af AI, selvom det under andre omstændigheder, f.eks. ved brug af andre teknologier, ikke nødvendigvis ville være tilfældet.”

Derudover fremgår følgende af afsnit 2.2.2.1. af udkastets almindelige bemærkninger:

> ”Datatilsynet har i flere sager taget stilling til kravene til det supplerende retsgrundlag ved offentlige myndigheders brug af kunstig intelligens. Der har herved udviklet sig en særlig praksis for brugen af AI-løsninger, hvorefter der i visse tilfælde stilles krav om et klarere supplerende retsgrundlag, end hvad der nødvendigvis ville gælde ved brug af andre teknologier [Datatilsynets fremhævning].”

Der er i den forbindelse henvist til en konkret sag hos Datatilsynet (med j.nr. 2023-212-0015) om, hvorvidt Københavns Kommunes havde hjemmel til udvikling og anvendelse af et AI-system indenfor sundheds- og omsorgsområdet.

Datatilsynet kan konstatere, at væsentlige elementer i tilsynets udtalelse **ikke** fremgår af afsnittet. Datatilsynet bemærkede således bl.a. i den pågældende udtalelse til Københavns Kommune, at det ikke nødvendigvis vil være forudsigeligt og gennemsigtigt for borgeren, at dennes potentielle behov for og gavn af træning og rehabilitering vurderes ved brug af en AI-løsning. Derudover fremgik det af udtalelsen, at det måtte tillægges vægt, at den målgruppe, kommunen ønskede at behandle oplysninger om – borgere, som helbredsmæssigt befinder sig i en situation, som nødvendiggør en vurdering af et potentielt behov for træning med henblik på at undgå funktionsnedsættelse – var en sårbar målgruppe.

Endvidere undersøgte Datatilsynet ikke kun bestemmelserne i serviceloven i den konkrete sag men også forarbejderne til bestemmelserne i forhold til, om rækkevidden af den pågældende behandling af personoplysninger, der kan ske for at udføre de pågældende opgaver, var omtalt, herunder om – og i hvilket omfang – der kunne behandles personoplysninger på den måde, som det ville være tilfældet ved brug af den pågældende AI-løsning. De pågældende bestemmelser i serviceloven havde efter Datatilsynets vurdering karakter af bestemmelser, som alene overordnet forpligtede kommuner til at udføre bestemte opgaver og i den forbindelse forudsatte behandling af personoplysninger med henblik på udførelse af disse opgaver.

I den ovenfor omtalte sag lagde Datatilsynet således vægt på den store mængde personoplysninger og karakteren af personoplysningerne, der ofte sker behandling af ved brug af AI-systemer. Derudover lagde Datatilsynet vægt på, at AI-systemet skulle anvendes som beslutningsstøtte, hvor myndigheden skulle handle ud fra en forudsigelse fra systemet om den enkelte borger og dermed påvirke borgerens helbredsmæssige situation. I den forbindelse var Datatilsynet opmærksom på risikoen for automation bias, som også er nærmere omtalt i det tidligere fremsendte høringssvar fra tilsynet. Datatilsynet lagde endelig også vægt på, hvordan personoplysningerne skulle behandles. I den forbindelse bemærkede Datatilsynet, at brug af AI medfører bl.a., at AI-systemerne kan lære, finde sammenhænge og gennemføre sandsynlighedsanalyser og drage konklusioner langt ud over det, som en fysisk sagsbehandler ville være i stand til.

Der var i den konkrete sag således en række omstændigheder, der havde betydning for, at Datatilsynet vurderede, at der var krav om et klart supplerende retsgrundlag til behandlingen af personoplysninger i forbindelse med anvendelsen af det pågældende AI-system i drift.

Endvidere afhænger kravet til klarheden af det supplerende retsgrundlag generelt af, hvor indgribende behandlingen af personoplysninger vil være for borgerne. Der henvises i den forbindelse til afsnit 4.2. i Datatilsynets tidligere høringssvar. I vurderingen bør det bl.a. indgå, hvilke oplysninger der behandles og om hvilke personer, herunder f.eks. sårbare borgere, ligesom omfanget af personoplysninger også er relevant at inddrage. Retsgrundlaget bør efter Datatilsynets opfattelse også vurderes ud fra, hvor direkte og indgribende f.eks. en afgørelse eller aktivitet er for borgerne. Det gælder, uanset om aktiviteten er bebyrdende eller begunstigende for borgerne. Derfor stilles der efter Datatilsynets opfattelse forskellige krav til klarheden af det relevante retsgrundlag til behandling af personoplysninger i forbindelse med henholdsvis udvikling og drift af en løsning. [8]

Det bør også indgå i vurderingen, hvordan personoplysningerne behandles. F.eks. er samkøring af personoplysninger i kontroløjemed og profilering behandlingsaktiviteter, der anses for særligt indgribende, og hvor der derfor er et krav om et klart retsgrundlag. Det gør sig også gældende, hvis der er tale om profilering til brug for beslutningsstøtte, hvor det ikke er med henblik på at træffe automatiske afgørelser.

Det kan derfor være relevant, hvilken teknologi der anvendes, hvis det har betydning for f.eks. omfanget af personoplysninger der behandles, og/eller måden oplysningerne behandles på.

5.4. I afsnit 2.2.2.1. i udkastets almindelige bemærkninger er der i forhold til det tidligere fremsendte udkast tilføjet en beskrivelse af, at der er behandlingsaktiviteter, der foretages ved brug af AI-systemer, og som efter en konkret vurdering ikke anses for indgribende overfor de registrerede. I den forbindelse fremgår det, at disse behandlingsaktiviteter ikke vil være underlagt

8 Der henvises til afsnit 5.2.2 i Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens (oktober 2023)

et krav om et yderligere klart og præcist supplerende retsgrundlag. Udkastet oplister eksempler på sådanne typer systemer. I den forbindelse nævnes AI-systemer, der anvendes til effektivisering i forbindelse med journalisering, mødeindkaldelser, formatskifte (tale-til-tekst) eller referatskrivning.

Datatilsynet bemærker i den forbindelse, at behandling af personoplysninger i forbindelse med anvendelse af AI til formatskifte (tale-til-tekst) eller referatskrivning alt efter omstændighederne kan være indgribende for borgerne. Det afhænger af de ovenfor nævnte omstændigheder i afsnit 5.3, herunder de omstændigheder, der er omtalt i den ovenfor nævnte udtalelse fra Datatilsynet til Københavns Kommune.

5.5. Det følger af udkastets bemærkninger til § 3, stk. 1, at bestemmelsen ikke vil kunne fungere som hjemmel til, at myndigheder og organer kan behandle nye personoplysninger. Datatilsynet forstår på bemærkningerne, at bestemmelsen alene vil kunne fungere som et supplerende retsgrundlag for behandling af personoplysninger, som myndigheder og organer i forvejen foretager efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, og myndighedens supplerende retsgrundlag for behandlingen af personoplysninger i forbindelse med den pågældende myndighedsudøvelse. Datatilsynet forstår på den baggrund, at udkastets § 3, stk. 1, ikke giver adgang til at indsamle nye oplysninger om borgerne til brug for f.eks. profilering i forbindelse med udvikling og anvendelse af AI-systemer, der skal understøtte myndighedernes og organernes opgavevaretagelse.

5.6. Det følgende fremgår af udkastets afsnit 3:

> Det er Forsknings-, Uddannelses- og Digitaliseringsministeriets vurdering, at der generelt kan være en række potentialer forbundet med myndighedernes og organernes anvendelse af AI-systemer, der f.eks. kan bidrage til at gøre den offentlige sektor bedre for borgere og virksomheder samt gøre den offentlige sektor mere effektiv. Det gælder såvel i forbindelse med sagsbehandling som i opgavevaretagelsen i sin helhed – både i forhold til anvendte ressourcer og i løftet af kvaliteten i disse opgaver. Behandlingen kan derfor anses for at ske af hensyn til væsentlige samfundsinteresser og som led i myndighedsudøvelse.
>
> Lovforslaget skal på den baggrund anses for at udgøre det supplerende retsgrundlag for behandling af personoplysninger ved udvikling og anvendelse af AI-systemer i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra e, artikel 9, stk. 2, herunder litra g, og artikel 10.

Det er Datatilsynets opfattelse, at det kunne fremgå klarere af lovudkastets bestemmelser, hvilke typer oplysninger der omfattes af det supplerende retsgrundlag. Artikel 6, stk. 1, litra e, er nævnt i udkastets § 1 om lovens anvendelsesområde, og det kunne umiddelbart opfattes som om, at behandling af særlige kategorier af oplysninger omfattet af artikel 9 eller personoplysninger vedrørende straffedomme og lovovertrædelser omfattet af artikel 10 ikke er omfattet af reguleringen i lovudkastet. Datatilsynet er opmærksom på, at personoplysninger omfattet af artikel 9 og artikel 10 er nævnt i lovudkastets § 3, stk. 2, men det kunne ikke desto mindre overvejes, om det i relation til anvendelsesområdet i § 1 kan tydeliggøres, at reguleringen i lovudkastet omfatter alle typer af personoplysninger. Det bemærkes i den forbindelse, at behandling af oplysninger om personnummer er særskilt reguleret i databeskyttelseslovens § 11.

En fravigelse af forbuddet mod behandling af særlige kategorier af personoplysninger i databeskyttelsesforordningens artikel 9, stk. 1, efter forordningens artikel 9, stk. 2, litra g forudsætter – som det er tilfældet med artikel 6, stk. 1, litra e – at der foreligger et supplerende retsgrundlag. Som det også fremgår af afsnit 2.2.1.1.2. i udkastets almindelige bemærkninger, er det Datatilsynets opfattelse, at dataansvarlige, der behandler særlige kategorier af personoplysninger omfattet af forbuddet i databeskyttelsesforordningens artikel 9, stk. 1, skal kunne

identificere en undtagelse til dette forbud i enten forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører forordningens artikel 9, *og* et lovligt grundlag for behandling i forordningens artikel 6. [9]

Der er i afsnit 2.2.1.1.2 i udkastets almindelige bemærkninger henvist til databeskyttelseslovens § 8, stk. 1, i forhold til behandling af oplysninger om strafbare forhold. Datatilsynet skal i den forbindelse henvise til sit høringssvar til det tidligere fremsendte udkast til lovforslag. Her bemærkede tilsynet, at i det omfang der er hjemmel til behandling af oplysninger om strafbare forhold i anden lovgivning, skal der ikke derudover være hjemmel i databeskyttelseslovens § 8. I den forbindelse henviste tilsynet til databeskyttelseslovens § 1, stk. 3, hvoraf det fremgår, at regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reglerne i databeskyttelsesloven.

5.7. Det følger af udkastets § 3, stk. 2, at vedkommende minister på eget ressort *kan* fastsætte passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser i forbindelse med behandling omfattet af stk. 1, når behandlingen omfatter personoplysninger omfattet af databeskyttelsesforordningens arti kel 9, stk. 1, eller artikel 10 herunder hvis sådanne foranstaltninger er på krævet i henhold til databeskyttelsesreglerne.

Det følger af stk. 3 i bestemmelsen, at Domstolsstyrelsen kan fastsætte de i stk. 2 nævnte foranstaltninger i forbindelse med domstolenes behandling omfattet af stk. 1.

I det tidligere fremsendte udkast til lovforslag fremgik det af bestemmelsen, at vedkommende minister på eget ressort *skal* fastsætte passende og specifikke foranstaltninger.

I forhold til vurdering af, om det er nødvendigt at fastsætte yderligere foranstaltninger fremgår det følgende af udkastets bemærkninger til bestemmelsen:

> ”Ved vurderingen af, om det efter databeskyttelsesreglerne er nødvendigt at fastsætte yderligere foranstaltninger, vil det være relevant at overveje, om der allerede følger passende og specifikke foranstaltninger af den relevante særlovgivning, som finder anvendelse på den pågældende behandling. I visse sektorer kan der f.eks. allerede være fastsat særlige regler eller foranstaltninger, der indeholder passende garantier for beskyttelsen af den registreredes rettigheder og interesser i forbindelse med sektorens øvrige behandling af personoplysninger. Det er også muligt, at der allerede er taget højde for sådanne passende og specifikke foranstaltninger for den registreredes rettigheder og interesser på anden vis, f.eks. ved individuelle dataansvarliges databehandlingspolitikker og lignende. I sådanne tilfælde vil der kunne være begrænset behov for at fastsætte yderligere foranstaltninger i forbindelse med anvendelsen af et AI-system til den pågældende behandling i en bekendtgørelse. Det er dog væsentligt at bemærke, at der bør tages højde for, hvorvidt sådanne foranstaltninger adresserer de specifikke risici, der ses ved brugen af det konkrete AI-system, når der foretages en vurdering af, hvorvidt foranstaltningerne er tilstrækkelige.”

Derudover fremgår det, at den foreslåede bestemmelse vil etablere en bemyndigelsesbestemmelse som for de enkelte ressortministre vil være mulig at anvende enten konkret i forhold til bestemte AI-systemer eller til at fastsætte en mere generel ramme for brugen af AI-systemer inden for et givent sektorområde. Herefter fremgår det, at bekendtgørelsen kan indeholde oplysninger, som forventeligt allerede vil være identificeret som led i den dataansvarliges udarbejdelse af en konsekvensanalyse vedrørende databeskyttelse efter databeskyttelsesforordningens artikel 35.

9 Der henvises til Datatilsynets udtalelse af 7. november 2019 om behandling af følsomme oplysninger, der er tilgængelig på tilsynets hjemmeside: Behandling af følsomme oplysninger

Det fremgår af bemærkningerne til bestemmelsen i udkastet, at det ved vurderingen af, om der bør fastsættes yderligere foranstaltninger i medfør af udkastets § 3, stk. 2, vil være relevant at tage hensyn til, hvorvidt passende og specifikke foranstaltninger kan være nødvendige grundet omkringliggende omstændigheder, der gør behandlingen af personoplysninger mere indgribende. I den forbindelse er der som eksempel nævnt tilfælde, hvor der behandles personoplysninger om sårbare personer og grupper af personer.

Datatilsynets forstår dog også, at Forsknings-, Uddannelses-, og Digitaliseringsministeriet er opmærksom på, at databeskyttelsesforordningen allerede indeholder forpligtelser til f.eks. at sikre et tilstrækkeligt sikkerhedsniveau for behandlingen af personoplysninger. Det fremgår af bemærkningerne, at der ikke med bestemmelsen etableres yderligere forpligtelser for ressortministrene end, hvad der allerede følger af databeskyttelsesreglerne, men at den foreslåede bestemmelse i stedet vil bidrage til, at der skal stilles konkrete og nuancerede garantier, som vil afhænge af den konkrete behandling og formålet hermed.

Datatilsynet bemærker i den forbindelse, at det i praksis kan blive vanskeligt at vurdere for de enkelte ressortministre, om der er behov for at fastsætte foranstaltninger og betingelser for behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9 og 10 i en bekendtgørelse, hvis det skal ske på baggrund af en vurdering af, om de dataansvarlige selv har implementeret tilstrækkelige foranstaltninger. Det skyldes, at der på nogle sektorområder er flere forskellige offentlige myndigheder og organer, der er dataansvarlige for behandling af personoplysninger. Det gælder f.eks. på det sociale område, hvor 98 kommuner er dataansvarlige for hver deres behandling af personoplysninger inden for deres myndighedsområde.

Forsknings-, Uddannelses- og Digitaliseringsministeriets kan i stedet overveje, om § 3, stk. 2, skal indeholde krav om, at ressortministrene *skal* fastsætte formål, betingelser og foranstaltninger, der som minimum skal overholdes af de dataansvarlige i forhold til behandling af personoplysninger i forbindelse med udvikling og/eller anvendelse af AI-systemer, som indebærer en høj risiko for de registrerede. En sådan forpligtelse kan eventuelt begrænses til at finde anvendelse i de tilfælde, hvor der ikke i forvejen findes sådanne regler i lov eller bekendtgørelse på det pågældende sektorområde.

Som bemærket i Datatilsynets tidligere høringssvar kan der være andre forhold end oplysningernes karakter, der medfører, at behandling af personoplysninger i forbindelse med udvikling og/eller anvendelse af AI-systemer er mere indgribende. Der kan f.eks. være tale om behandling af oplysninger om sårbare personer eller behandling af fortrolige oplysninger som f.eks. personnumre eller adresser for personer med navne- og adressebeskyttelse, der ikke er omfattet af databeskyttelsesforordningens artikel 9 eller 10.

Det fremgår af udkastets bemærkninger til bestemmelsen, at med bestemmelsen vil offentlige myndigheder og organer blive ansvarlige for at overveje behovet for at behandle disse kategorier af personoplysninger. Datatilsynet bemærker i den forbindelse, at en sådan forpligtelse allerede følger af databeskyttelsesforordningens regler, herunder forordningens artikel 5, stk. 1, litra c, og undtagelserne i artikel 9, stk. 2, til at behandle særlige kategorier af oplysninger.

5.8. Det fremgår af afsnit 2.2.2.1 i udkastets almindelige bemærkninger, at formålet med den foreslåede ordning er at skabe et generelt nationalt retsgrundlag for de behandlingsaktiviteter, der foretages ved brug af AI-systemer. Det fremgår af afsnittet, at det skal gælde for både de behandlingsaktiviteter, der foretages ved brug af AI-systemer, der må anses for indgribende, samt de behandlingsaktiviteter, der ikke er indgribende.

Da databeskyttelsesreglerne er teknologineutrale, er det behandlingens karakter, omfang, sammenhæng og formål samt de risici behandlingsaktiviteterne udgør for de registrerede, der som hovedregel udgør rammen for de databeskyttelsesretlige regler.

Datatilsynet bemærker, at det i udkastet derimod er anvendelsen af en bestemt teknologi (AI) og dermed ikke konkrete myndighedsopgaver (formålet) og den konkrete behandling af personoplysninger, der er relateret hertil, som er det centrale.

Denne tilgang medfører efter Datatilsynets opfattelse, at det er mange forskelligartede behandlingsscenarier, som udkastet skal forsøge at regulere, når det skal omfatte alle offentlige myndigheders og organers behandlingsaktiviteter i forbindelse med udvikling eller anvendelse af AI-systemer i alle sammenhænge, hvor det skal understøtte myndighedsopgaver. Det kan derfor være vanskeligt alene på baggrund af udkastets bestemmelser at tilvejebringe et klart og præcist retsgrundlag for særligt de behandlingsaktiviteter, der er indgribende for borgerne. Dette er på trods af, at intentionen med udkastet til lovforslag ikke giver anledning til tvivl.

Det er Datatilsynets opfattelse, at den foreslåede ordning vil indebære, at offentlige myndigheder og organer ved vurderingen af deres supplerende retsgrundlag for behandlingsaktiviteter i forbindelse med udvikling og/eller anvendelse af AI-systemer, som er indgribende og dermed forventes at indebære en høj risiko for de involverede borgere (de registrerede), skal foretage en vurdering af bestemmelserne samt bemærkningerne i dette udkast til lovforslag, den eksisterende sektorlovgivning i forhold til de pågældende myndighedsopgaver og eventuelle bekendtgørelser på enkelte sektorområder, som udstedes i medfør af udkastets § 3, stk. 2 og 3.

6. Anvendelse af data fra myndighedernes historiske og lukkede sager

6.1. Det følgende fremgår af afsnit 2.2.1.1.3. i udkastets almindelige bemærkninger:

> ”Det følger af databeskyttelsesforordningens artikel 6, stk. 4, at når behandling til et andet formål end det, som personoplysningerne er indsamlet til, ikke er baseret på den registreredes samtykke eller EU-retten eller medlemsstaternes nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1, kan personoplysninger viderebehandles uden nyt retsgrundlag, hvis det nye formål er foreneligt med det formål, hvortil oplysningerne oprindeligt er indsamlet.”

Derudover fremgår det, at det dermed er muligt i national ret at fastsætte regler om viderebehandling af personoplysninger, og at sådanne regler skal tage hensyn til de mål, der fremgår af databeskyttelsesforordningens artikel 23, stk. 1. I den forbindelse er artikel 23, stk. 1, litra e, fremhævet som eksempel.

Datatilsynet ser i den forbindelse gerne, at ordlyden i artikel 6, stk. 4, gengives, og at der i den forbindelse også henvises til artikel 5, stk. 1, litra b, i databeskyttelsesforordningen, hvoraf det følger, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er uforenelig med disse formål.

Derudover ser Datatilsynet gerne, at det præciseres, at det er muligt at fastsætte nationale regler om viderebehandling af personoplysninger til et andet formål end det, som personoplysningerne er indsamlet til, og at sådanne regler skal udgøre en *nødvendig og forholdsmæssig foranstaltning* i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1.

Det følgende fremgår bl.a. om den foreslåede ordning i forhold til de dataansvarliges anvendelse af data fra historiske og lukkede sager i afsnit 2.2.2.1. i udkastets almindelige bemærkninger:

> ”Den foreslåede ordning vil desuden medføre, at personoplysninger vil kunne anvendes både til udvikling og til anvendelse af et AI-system. Dermed har offentlige myndigheder og organer mulighed for selv at udvikle eller få udviklet specialiserede AI-systemer, der er trænet på konkret og relevant træningsdata, herunder personoplysninger i myndighedens historiske og lukkede sager.”

Derudover fremgår det følgende af afsnit 2.2.2.3 i udkastets almindelige bemærkninger:

> ”Til dette bemærkes, at personoplysninger – der fremgår af historiske og lukkede sager – med fordel vil kunne anvendes til at udvide mængden af data, der kan anvendes i AI-systemers træningsdata med henblik på at forbedre og præcisere AI-systemers output. Dette vil særligt kunne løfte kvaliteten og pålideligheden af AI-systemernes output, da AI-systemerne typisk trænes til at kunne understøtte en specialiseret opgave. Derfor vil det være relevant for myndighederne og organerne at kunne anvende personoplysninger fra historiske og lukkede sager til at udvikle AI systemer, der eksempelvis skal anvendes til beslutningsstøtte i lignende op gaver.”

Datatilsynet har noteret sig, at det i det nye udkast fremgår af afsnit 2.2.2.3., at myndighederne og organerne udelukkende vil have adgang til at anvende personoplysninger fra historiske og lukkede sager, som myndighederne og organerne på tidspunktet for udviklingen opbevarer, herunder oplysninger der endnu ikke er aflevereret til et offentligt arkiv. Derudover fremgår det, at myndighederne og organerne ikke vil have mulighed for at genindhente personoplysninger fra et offentligt arkiv, når kopier af personoplysninger allerede er slettet i myndighedernes og organernes interne databaser.

Datatilsynet bemærker i den forbindelse, at de dataansvarlige offentlige myndigheder og organer er forpligtede til at slette eller anonymisere oplysninger, når de ikke længere er nødvendige at behandle i forhold til formålet med behandlingen af personoplysninger.[10] Hvis der fortsat behandles personoplysninger, selvom de burde have været slettet eller anonymiseret, f.eks. hvis der opbevares en kopi af materiale, der er afleveret til et offentligt arkiv, kan disse oplysninger efter Datatilsynets opfattelse ikke anvendes til udvikling af et AI-system til brug for den pågældende myndigheds opgavevaretagelse.

Derudover fremgår det, at hjemlen til viderebehandling bør afgrænses til viderebehandling af de personoplysninger, som de respektive myndigheder og organer allerede er eller vil komme i besiddelse af som led i deres opgavevaretagelse. Det fremgår i den forbindelse, at en generel hjemmel til viderebehandling af personoplysninger ikke vil kunne omfatte udveksling af personoplysninger mellem offentlige myndigheder og organer efter den foreslåede ordning.

Det følgende fremgår derudover af afsnit 2.2.2.3. i udkastets almindelige bemærkninger:

> ”Den foreslåede ordning vil medføre, at der vil blive etableret et grundlag for viderebehandling af personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 4, som myndigheden allerede er i besiddelse af og har lovlig adkomst til, hvilket dermed omfatter personoplysninger fra historiske og lukkede sager. Det skyldes, at den foreslåede ordning klart og tydeligt vil angive, at der vil kunne ske udvikling af AI-systemer på baggrund af per sonoplysninger, som myndigheden (i forvejen) behandler.
>
> Formålet med den foreslåede ordning er at undgå behovet for, at ressortministrene vil skulle tilvejebringe et særskilt retsgrundlag for viderebehandling af de personoplysninger, som myndighederne og organerne i forvejen er eller vil komme i besiddelse af og har lovlig adkomst til, samt at myndighederne og organerne ikke vil skulle foretage en forenelighedstest i henhold til databeskyttelsesforordningens artikel 6, stk. 4, før myndighederne og organerne vil kunne viderebehandle personoplysninger i historiske og lukkede sager til udvikling af AI-systemer.”

10 Det følger af databeskyttelsesforordningens artikel 5, stk. 1, litra e.

Datatilsynet henviser i den forbindelse til afsnit 5 i tilsynets tidligere høringssvar, hvor databeskyttelsesforordningens artikel 6, stk. 4, og artikel 23, stk. 1, er omtalt.

Forsknings-, Uddannelses-, og Digitaliseringsministeriet ses fortsat ikke i det nye udkast at have forholdt sig til, om loven vil udgøre en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er oplistet i artikel 23, stk. 1.

Det står derfor fortsat ikke Datatilsynet klart, hvilke af de hensyn, der er oplistet i artikel 23, stk. 1, litra a-j, der kan begrunde, at det er en nødvendig og forholdsmæssig foranstaltning, at alle de offentlige myndigheder og organer, som reglerne skal gælde for, i alle sammenhænge kan viderebehandle oplysninger fra historiske og afsluttede sager til brug for udvikling af AI-systemer.

Derfor er det Datatilsynets opfattelse, at det er nødvendigt, at de enkelte dataansvarlige offentlige myndigheder og organer skal foretage en vurdering i medfør af artikel 6, stk. 4, i forhold til, om personoplysninger, som er indsamlet til andre formål, herunder fra myndighedens lukkede og arkiverede sager, vil kunne anvendes til udvikling af AI-systemer, der skal understøtte deres opgavevaretagelse.

Efter Datatilsynets opfattelse har offentlige myndigheder – under iagttagelse af de forvaltningsretlige principper om saglighed og ligebehandling – et vidt skøn med hensyn til, i hvilket omfang myndigheden kan genbruge egne data som led i myndighedsudøvelsen. Det forudsætter imidlertid, at myndigheden foretager en konkret vurdering af, om brugen af de identificerede datasæt er forenelig med det formål, som dataene oprindeligt blev indsamlet til.

6.2. Det fremgår af afsnit 2.2.1.1.3. i udkastets almindelige bemærkninger, at behandling af personoplysninger til andre formål end de(t) oprindelige formål medfører, at borgerne skal oplyses om de(t) nye formål. Der er i den forbindelse henvist til artikel 13, stk. 3, og artikel 14, stk. 4. I den forbindelse fremgår det, at dataansvarlige i visse tilfælde kan være undtaget fra oplysningspligten. Der er i den forbindelse henvist til artikel 13, stk. 4, og 14, stk. 5.

I medfør af artikel 14, stk. 5, litra a, finder oplysningspligten efter henholdsvis artikel 14 ikke anvendelse, hvis den registrerede allerede er bekendt med oplysningerne. Derudover følger det af artikel 14, stk. 5, litra c, at oplysningspligten efter artikel 14 ikke finder anvendelse hvis og i det omfang indsamling eller videregivelse udtrykkelig er fastsat i EU-ret eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som fastsætter passende foranstaltninger til beskyttelse af den registreredes legitime interesser.

I databeskyttelsesforordningens præambelbetragtning nr. 50 er behandling af personoplysninger til andre formål end de, som oplysningerne oprindeligt er indsamlet til, også beskrevet. Heraf fremgår det bl.a., at når behandlingen er baseret på EU-retten eller medlemsstaternes nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund med henblik på at beskytte navnlig vigtige målsætninger af generel samfundsinteresse, bør den dataansvarlige kunne viderebehandle personoplysningerne uafhængigt af formålenes forenelighed. Det fremgår herefter, at de principper, der fastsættes i databeskyttelsesforordningen, og navnlig information til den registrerede om disse andre formål og om vedkommendes rettigheder, herunder retten til at gøre indsigelse, under alle omstændigheder bør sikres.

Det er Datatilsynets opfattelse, at kravet om udtrykkelighed indebærer, at det ikke må give anledning til tvivl, hvorvidt det i lovgivningen er fastsat, at den dataansvarlige skal foretage indsamling eller videregivelse af de pågældende personoplysninger.[11]

Derudover indebærer kravet om udtrykkelighed efter Datatilsynets opfattelse, at der skal være tale om en egentlig forpligtelse til at indsamle eller videregive oplysninger, ligesom det af de af EU-retten eller de nationale regler skal fremgå, hvilke oplysninger der skal indsamles eller videregives. Dette skyldes, at det i disse tilfælde vil være klart for den registrerede, at der vil blive indsamlet eller videregivet oplysninger om vedkommende og hvilke oplysninger.

Det vil således ikke være tilstrækkeligt, at lovgivningen alene hjemler en mulighed til at indsamle eller videregive oplysninger, da det ikke efter en sådan bestemmelse vil være klart for de registrerede, bl.a. at der vil blive registreret eller videregivet oplysninger og hvilke oplysninger.

Datatilsynet er af den opfattelse, at betingelserne i artikel 14, stk. 5 litra c – som en undtagelse til den generelle hovedregel om at iagttage oplysningspligten – skal fortolkes relativt strengt, og den påberåbte nationale lovgivning derfor skal medføre, at det beskyttelsesniveau som sikres ved databeskyttelsesforordningens artikel 14, stk. 1-4, ikke undermineres.[12]

7. Undtagelse til de registreredes rettigheder

7.1. Det fremgår af udkastets § 4, 1. pkt., at vedkommende minister kan fastsætte regler om, at bestemmelserne i databeskyttelsesforordningens artikel 12 og artikel 15-21 kan begrænses helt eller delvist, hvis ét af forholdene i databeskyttelsesforordningens artikel 23, stk. 1, gør sig gældende. Herefter fremgår det, at regler udstedt i medfør af 1. pkt. skal indeholde, hvor det er relevant, specifikke bestemmelser vedrørende de forhold, som fremgår af databeskyttelsesforordningens artikel 23, stk. 2.

Det følgende fremgår af afsnit 2.3.2.1. i udkastets almindelige bemærkninger:

> ”Det er Forsknings-, Uddannelses- og Digitaliseringsministeriets vurdering, at en mulighed for helt eller delvist at kunne begrænse den registreredes rettigheder er relevant i forbindelse med offentlige myndigheders og organers udvikling og anvendelse af AI-systemer. AI-systemer er ofte kendetegnet ved komplekse datastrukturer, hvor oplysninger fra mange registrerede potentielt vil indgå i træningsdata. Det vil ikke altid være muligt at udskille de registreredes personoplysninger fra modelparametrene. Dermed kan AI systemernes funktionsmåde gøre det vanskeligt, eller i visse tilfælde sågar umuligt, for myndighederne og organerne at håndtere de registreredes rettigheder, når først personoplysningerne er indlejret i et AI-system. Dette gælder f.eks. retten til sletning eller retten til indsigt, der grundet vanskeligheden i at fremfinde eller adskille data er vanskelige at imødekomme.”

Derudover fremgår det følgende af afsnit 3.1. i udkastets almindelige bemærkninger:

> ”Et AI-system vil i sin natur potentielt kunne medføre en begrænsning af den registreredes rettigheder, f.eks. hvis AI-systemets funktionsmåde vil kunne stille den registrerede dårligere i forhold til vedkommendes rettigheder, f.eks. i forhold til retten til indsigt eller sletning. Det skyldes, at AI-systemer ofte er kendetegnet ved komplekse datastrukturer, hvor oplysninger fra mange registrerede indgår i trænings- og modelleringsteknikker. Det vil ikke altid være muligt at udskille de registreredes personoplysninger fra modelparametrene. Det betyder, at den registreredes rettigheder, herunder f.eks. retten til indsigt og retten til sletning, i praksis kan være vanskelig – eller

11 Justitsministeriet, Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, Betænkning nr. 1565, Del I, bind 1, s. 300-301.
12 EU-Domstolens dom af 28. november 2024 i C-169/23 Másdi, præmis 54

> i visse tilfælde umulig – at opfylde, når oplysningerne først er integreret i et AI-system."

I udkastets bemærkninger til § 4, stk. 1, er det anført, at bestemmelsen vil være med til at effektivisere udviklingen, videreudviklingen og anvendelsen af AI-systemer. Det er begrundet med, at AI-systemer efter deres natur potentielt vil kunne medføre en begrænsning af den registreredes rettigheder på grund af AI-systemers komplekse opbygning.

Datatilsynet henviser til bemærkningerne ovenfor i afsnit 2.1. om de dataansvarliges forpligtelser, der følger af databeskyttelsesforordningens artikel 25, stk. 1, om databeskyttelse gennem design. I den forbindelse bemærkes det, at det forud for behandlingen af personoplysninger skal vurderes, om databeskyttelsesreglerne i praksis kan overholdes med den løsning og det design, der ønskes anvendt. Det gælder også reglerne om de registreredes rettigheder i artikel 12 og artikel 15-21.

7.2. Datatilsynet har noteret sig, at der i afsnit 2.3.2.1. i udkastets almindelige bemærkninger er tilføjet en forudsætning om, at ressortministrenes mulighed for at indføre en undtagelse til de registreredes rettigheder (enten generelt på ressortområdet eller for behandlingen af personoplysninger i forbindelse med brugen af et specifikt AI-system) vil skulle ske med afsæt i de hensyn, som følger af databeskyttelsesforordningens artikel 23, stk. 1.

Det følgende fremgår af afsnit 2.3.2.1. i udkastets almindelige bemærkninger:

> "Dermed vil den foreslåede ordning medføre, at relevante undtagelser vil kunne fastsættes på de ressortområder, hvor det efter en konkret vurdering er vurderet relevant, samt at betingelserne for en undtagelse efter databeskyttelsesforordningens artikel 23, stk. 1, er opfyldt."

Datatilsynet har noteret sig, at det er tilføjet i det nye udkast, at databeskyttelsesforordningens artikel 23, stk. 1, har et snævert anvendelsesområde, hvorfor det ikke i alle tilfælde vil være muligt at gøre undtagelse til den registreredes rettigheder med hjemmel i databeskyttelsesforordningens artikel 23, stk. 1.

7.3. Forsknings-, Uddannelses- og Digitaliseringsministeriet ses også i det nye udkast at have henvist til artikel 23, stk. 1, litra e, som eksempel på et af de hensyn i artikel 23, stk. 1, som efter ministeriets vurdering er nærliggende at vurdere.

Datatilsynet kan konstatere, at der i det nye udkast er tilføjet en henvisning til de retningslinjer fra Det Europæiske Databeskyttelsesråd (EDPB), som tilsynet henviste til i sit tidligere høringssvar.

Datatilsynet skal henvise til afsnit 6 i tilsynets tidligere fremsendte høringssvar, hvor det nationale råderum i artikel 23, herunder særligt artikel 23, stk. 1, litra e, bl.a. er omtalt.

Det er som nævnt i Datatilsynets tidligere høringssvar tilsynets opfattelse, at der stilles krav om betydelig klarhed ved ethvert nationalt grundlag, der begrænser de registreredes rettigheder. Det står derfor fortsat ikke Datatilsynet klart, hvordan de enkelte ressortministre i praksis vil kunne fastsætte regler i bekendtgørelser på deres respektive ressortområde med den fornødne klarhed, og som forholder sig til hensynene i artikel 23, stk. 1.

8. Øvrige bemærkninger

8.1. Det følgende fremgår af afsnit 2.2.1.1. i udkastets almindelige bemærkninger:

> ”[...] Det indebærer bl.a., at offentlige myndigheder og organer skal bestræbe sig på at udvikle AI-systemer, der understøtter beskyttelsen af personoplysninger ved at integrere passende tekniske eller organisatoriske foranstaltninger.
>
> Herudover følger det bl.a. af databeskyttelsesforordningens præambelbetragtning nr. 38, at børn generelt bør nyde særlig beskyttelse af deres personoplysninger, eftersom de ofte er mindre bevidste om de pågældende risici, konsekvenser og garantier og deres rettigheder for så vidt angår behandling af personoplysninger. Dermed bør offentlige myndigheder og organer udvise tilstrækkelig forsigtighed og ansvarlighed, når disse behandler personoplysninger om børn.”

Datatilsynet bemærker generelt, at de dataansvarlige offentlige myndigheder og organer skal sikre (og ikke blot skal bestræbe sig på) et sikkerhedsniveau, der passer til de risici, som en given behandling af personoplysninger indebærer. Det indebærer, at de dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger, hvor der tages hensyn til en række omstændigheder, der er nævnt i databeskyttelsesforordningens artikel 32, stk. 1.

Derudover bemærker Datatilsynet, at de dataansvarlige offentlige myndigheder og organer skal udvise tilstrækkelig forsigtighed og ansvarlighed ved behandling af oplysninger om alle personer. Børn nyder imidlertid som anført i udkastet en særlig beskyttelse. Det indebærer, at de dataansvarlige skal være særligt opmærksomme, hvis de behandler oplysninger om børn, da det bl.a. kan have betydning i forhold til de dataansvarliges risikovurdering af de pågældende behandlingsaktiviteter, samt hvordan der sikres gennemsigtighed.

8.2. I afsnit 2.1.1.1. i udkastets almindelige bemærkninger, som bl.a. vedrører udkastets anvendelsesområde, er forholdet til retshåndhævelsesloven beskrevet. Datatilsynet skal i den forbindelse henvise til tilsynets tidligere fremsendte høringssvar, hvor tilsynet bemærkede, at retshåndhævelsesloven ikke regulerer behandling af personoplysninger udover reglerne i databeskyttelsesforordningen og databeskyttelsesloven, som det også fremgår i dette udkast. Det er derimod regler, der finder anvendelse på behandling af personoplysninger, der ikke er omfattet af databeskyttelsesforordningen og databeskyttelsesloven.

8.3. I afsnit 2.2.1.1.2. i udkastets almindelige bemærkninger om behandling af bl.a. særlige kategorier af personoplysninger er databeskyttelsesforordningens artikel 9, stk. 2, litra a-c og e-g, fremhævet som særligt relevante.

Det følger af databeskyttelsesforordningens artikel 9, stk. 2, litra a, at forbuddet mod at behandle de særlige kategorier af personoplysninger, der er omfattet af artikel 9, stk. 1, ikke finder anvendelse, hvis den registrerede har givet udtrykkeligt samtykke til behandling af sådanne oplysninger.

Datatilsynet skal generelt bemærke, at en offentlig myndighed sædvanligvis ikke vil kunne behandle personoplysninger på baggrund af et samtykke, fordi betingelserne for et gyldigt samtykke kan være vanskelige at opfylde, når en offentlig myndighed behandler personoplysninger. [13]

9. Afsluttende bemærkninger

Datatilsynet forudsætter at blive hørt i forbindelse med udarbejdelse af bekendtgørelser og lignende generelle forskrifter, som knytter sig til lovudkastet, jf. databeskyttelseslovens § 28.

13 Der henvises til afsnit 5.2.3 i Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens (oktober 2023)

Kopi af dette brev er dags dato sendt til Justitsministeriets Lovafdeling til orientering.

Med venlig hilsen

Kristian Korfits Nielsen
Formand, Datarådet

Cristina Angela Gulisano
Direktør, Datatilsynet

Digitaliseringsstyrelsen
Landgreven 4
1301 København K

Sendt pr. mail til jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk og kahevi@digst.dk

12. oktober 2026

Dok. nr.: 26/25820-7

Sagsbehandler:
Line Kürstein

Domstolsstyrelsens høringssvar

Digitaliseringsstyrelsen har ved mail af 14. september 2026 anmodet Domstolsstyrelsen om eventuelle bemærkninger til udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven).

Domstolsstyrelsen har i den anledning følgende bemærkninger:

Det bør udtrykkeligt fremgå af bemærkningerne til § 1, at loven også omfatter domstolene i det omfang domstolene behandler personoplysninger efter artikel 6, stk. 1, litra e, i overensstemmelse med kravet i artikel 6, stk. 2, jf. stk. 3, i databeskyttelsesforordningen. Det kan fx være ved en tilføjelse herom i lovforslagets side 15 og side 59.

De anvendte begreber ”forvaltningsmæssige afgørelser” og ”faktisk forvaltningsvirksomhed” i bemærkningerne til § 2, nr. 4 (side 63-64) kan give indtryk af, at lovforslaget navnlig er rettet mod bestemte myndigheder. Bemærkningerne bør formuleres mere generelt og bør undgå særligt at fremhæve bestemte myndighedstyper eller opgavekategorier. En mere overordnet beskrivelse som fx ”afgørelser, der angår borgernes retsstilling” el.lign. vil bedre afspejle lovforslagets brede anvendelsesområde.

Det bør i bemærkningerne til § 3 præciseres, at lovforslaget ikke pålægger offentlige myndigheder og organer at udvikle eller anvende AI-systemer i forbindelse med udførelsen af deres lovbestemte opgaver. En sådan præcisering er væsentlig og vil bidrage til at understrege, at lovforslaget ikke tager stilling til, hvorvidt og i hvilket omfang AI skal anvendes i opgaveløsningen, men at lovforslaget alene etablerer en generel databeskyttelsesretlig hjemmel og et klart retsgrundlag for de offentlige myndigheder og organer, der vælger at udvikle eller anvende AI-systemer ved behandling af personoplysninger som led i deres opgavevaretagelse efter anden lovgivning.

Endelig kan det i de specielle bemærkninger til den foreslåede § 4 med fordel tydeliggøres, at udvikling eller anvendelse af AI-systemer ikke i sig selv kan føre til, at registrerede afskæres fra eller får indskrænket deres rettigheder. En sådan præcisering vil bidrage til at understrege

beskyttelsen af de registreredes rettigheder og interesser, som skal iagttages uanset den teknologiske kompleksitet, der måtte kendetegne det anvendte AI-system.

Med venlig hilsen

Laila Lindemark

Til Digitaliseringsstyrelsen

Forsknings-, Uddannelses- og Digitaliseringsministeriet

8. oktober 2026

Høringssvar til AI-hjemmelsloven

Udkast til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Edora A/S takker for muligheden for at afgive høringssvar til udkastet til AI-hjemmelsloven. Vi støtter ambitionen om et klart retsgrundlag for ansvarlig anvendelse af kunstig intelligens i den offentlige sektor.

Edora arbejder med digital suverænitet, IT-beredskab og resiliens i den digitale infrastruktur. Det omfatter blandt andet Edora Cloud og den danskudviklede, danskdriftede AI-tolkeløsning Let's Talk. Vores udgangspunkt er: Avanceret AI og reel kontrol over data og drift bør udvikles sammen.

Vi anbefaler, at lovforslaget styrkes på tre områder:

- **En uafhængig og AI-fri second opinion for borgeren;**
- **bindende krav til digital suverænitet og robust drift;**
- **og det offentlige som strategisk indkøber, der understøtter dansk og europæisk teknologisk kapacitet.**

1. Ret til en uafhængig, AI-fri second opinion

1.1. AI skal understøtte – ikke erstatte – det faglige ansvar

Edora ser et betydeligt potentiale i AI-baseret beslutningsstøtte. Teknologien kan efter vores vurdering frigøre tid, understøtte kvaliteten og gøre sagsbehandlingen mere effektiv. Lovudkastet omfatter beslutningsstøtte, men giver ikke i sig selv hjemmel til fuldautomatiske afgørelser omfattet af GDPR artikel 22. Denne grænse skal fastholdes.[1]

Det er positivt, at bemærkningerne kræver reel menneskelig stillingtagen. Udkastet anerkender samtidig risikoen for, at en sagsbehandler tillægger AI-systemets vurdering større vægt end sin egen. Dokumentation, logning og procedurer for afvigelse fra AI-anbefalinger omtales som mulige understøttende tiltag, men er ikke i sig selv gjort obligatoriske ved lovudkastet.[2]

Edora anbefaler derfor en udtrykkelig ret til, at borgeren kan få en afgørelse, hvor AI har indgået som beslutningsstøtte, vurderet på ny af et menneske i en funktion, der er uafhængig af den oprindeligt besluttende myndighed. Retten bør også overvejes ved andre væsentlige borgerrettede tiltag, med den nødvendige tilpasning til det enkelte område.

En efterfølgende second opinion må ikke blive en erstatning for reel menneskelig vurdering i første instans. Den er en yderligere retssikkerhedsgaranti.

[1] Lovudkastet, § 2, nr. 4 og 6, § 3 samt almindelige bemærkninger, pkt. 1.1, s. 7–8. Udkastets hjemmel omfatter ikke fuldautomatiske afgørelser efter GDPR artikel 22. Høringsmateriale.

[2] Lovudkastet, almindelige bemærkninger, pkt. 2.1.2, s. 18–19, og pkt. 2.2.1.1.1, s. 22, om reel menneskelig involvering og risikoen for at tillægge AI-vurderingen for stor vægt.

1.2. Sagens faktiske grundlag skal med – AI-vurderingen skal ikke

Det er ikke tilstrækkeligt at skifte sagsbehandler. Den nye vurdering skal være organisatorisk, funktionelt og informationsmæssigt adskilt fra den oprindelige AI-støttede vurdering.

Den uafhængige sagsbehandler skal arbejde ud fra sagens fulde relevante faktiske grundlag: borgerens ansøgning og bemærkninger, originale bilag, dokumenterede hændelser, faglige erklæringer og eventuelle nye, lovligt indhentede oplysninger. Materialet må ikke begrænses til de forhold, som det oprindelige AI-system udvalgte eller fremhævede.

Derimod skal AI-genererede anbefalinger, risikoscorer, profiler, sammenfatninger, udkast, konklusioner og begrundelser **ikke indgå i den sagspakke, der overføres til den uafhængige vurderingsfunktion**. Det samme gælder AI-vurderinger, der er kopieret ind i menneskeskrevne notater eller afgørelsestekster. **En ny dokumenttitel eller en menneskelig underskrift må ikke gøre AI-vurderingen til en del af det nye vurderingsgrundlag.**

Den nye sagsbehandler skal heller ikke anvende et andet AI-system til at vurdere sagens realitet. Opdraget bør beskrive det spørgsmål, der skal vurderes, uden at forelægge den oprindelige konklusion. Vurderingen og dens begrundelse skal dokumenteres selvstændigt.

Ordningen forudsætter derfor, at myndighederne fra begyndelsen kan adskille originale oplysninger fra AI-bearbejdning og dokumentere oplysningernes oprindelse. Et AI-resumé er ikke en erstatning for et originalt bilag. Hvor AI har omskrevet eller transskriberet oplysninger, skal der stilles krav om at det underliggende materiale skal være tilgængeligt eller oplysningerne verificeres uafhængigt.

1.3. Kommuner og Ankestyrelsen som konkrete modeller

Eksempel: Kommune A og kommune B. Kommune A træffer med AI-baseret beslutningsstøtte en afgørelse om en borgers ansøgning om hjælp. Borgeren anmoder om en second opinion. En kvalificeret sagsbehandler i kommune B modtager det relevante originale sagsgrundlag, men ikke AI-systemets vurderinger eller den oprindelige afgørelses begrundelse. Sagsbehandleren foretager en ny, konkret menneskelig vurdering efter det relevante retsgrundlag, hvor det er forbudt at anvende AI.

Det kan organiseres som en lovreguleret tværkommunal ordning med fælles faglige krav, habilitetsregler og uafhængig fordeling af sager. Det afgørende er borgerens ret til en anden, uafhængig vurderingsfunktion – ikke, at borgeren skal finde den kommune, der forventes at give det mest fordelagtige udfald. Direkte gensidige aftaler bør heller ikke skabe incitament til blot at bekræfte hinandens afgørelser.

Alternativ: En særskilt funktion i Ankestyrelsen. På de relevante sagsområder kan en fagligt og adgangsmæssigt adskilt funktion i Ankestyrelsen gennemføre den AI-frie vurdering. Det skal i så fald være en reel ny vurdering – ikke alene en kontrol af, om den oprindelige sagsbehandler har fulgt AI-anbefalingen korrekt.

Det er vigtigt at skelne denne ordning fra almindelig klagebehandling. Ankestyrelsens vejledning forudsætter, at kommunen sender afgørelse, klage, genvurdering og relevante sagsakter. En blindet second opinion kan derfor ikke gennemføres ved blot at udelade materiale fra en eksisterende klagesag.[3]

[3] Ankestyrelsen, vejledning til kommunernes ankeskema, afsnittet om sagsakter. Se også principafgørelse 96-17 om den oprindelige kommunes genvurdering. Den foreslåede tværkommunale ordning er en ny ordning, ikke en beskrivelse af gældende klageregler.

Edora foreslår **to adskilte prøvelsesspor**: En AI-fri vurdering af sagens realitet på originalt grundlag, og en særskilt kontrol af den oprindelige sagsbehandling, AI-anvendelse og begrundelse. AI-materialet skal bevares og være tilgængeligt for den kompetente kontrolfunktion, men ikke for den blindede vurderingsfunktion. Adgangen skal adskilles teknisk og organisatorisk, og den uafhængige vurdering skal afsluttes og registreres uden påvirkning fra kontrolsporet.

Adskillelse er ikke sletning eller hemmeligholdelse. Borgerens adgang til indsigt, mulighed for at forklare sig og mulighed for at dokumentere fejl i AI-anvendelsen må ikke forringes. Relevant materiale skal fortsat kunne indgå i lovlighedskontrol, tilsyn og domstolsprøvelse.

1.4. Tydelig hjemmel og en realistisk økonomisk vurdering

Der er tale om et forslag til en ny rettighed. Lovgiver skal fastlægge vurderingsfunktionens kompetence, behandlingsgrundlaget for overførsel af sagsakter, sagsfrister, finansiering og virkningen af en afvigende vurdering. Det skal eksempelvis være klart, hvornår en uoverensstemmelse udløser genoptagelse eller en bindende klageafgørelse. Ordningen må ikke forringe eksisterende klagemuligheder eller medføre, at borgeren mister en klagefrist. Lovudkastet etablerer ikke allerede en generel adgang til at udveksle sager mellem myndigheder.[4]

Ordningen kan umiddelbart forekomme ressourcekrævende. Edoras forventning er imidlertid, at de fleste afgørelser ikke vil blive begæret vurderet igen. Effektiviseringsgevinster ved bred anvendelse af AI kan derfor efter vores vurdering give plads til en grundig menneskelig vurdering i den mindre del af sagerne, hvor borgeren ønsker det. Vi forventer, at der fortsat kan opnås en betydelig samlet samfundsøkonomisk gevinst.[5]

Dette er en forventning, ikke en dokumenteret besparelse. Ministeriet bør beregne omkostninger og forventet anvendelse og følge op på både økonomi, sagsbehandlingstid og retssikkerhed. Retten bør være gebyrfri og let at benytte.

2. Genidentifikation skal vurderes i sammenhæng

Edora finder, at kravene til AI-drift skal tage udgangspunkt i den reelle risiko ved oplysningerne – ikke blot i, om navne og CPR-numre er fjernet. Oplysninger kan være personhenførbare gennem kombination med andre oplysninger. Fjernelse af direkte identifikatorer er derfor ikke i sig selv dokumentation for anonymitet.[6]

Sundhedsområdet: Kombinationen af, at en kvinde har født børn på to bestemte datoer og fået fjernet et modermærke på højre arm, kan indsnævre personkredsen meget betydeligt. Sammenholdt med andre tilgængelige oplysninger kan et sådant forløb muliggøre identifikation, selv om journaludtrækket ikke indeholder navn eller CPR-nummer.

Domstolsområdet: En dom med fjernede navne kan fortsat indeholde en kombination af datoer, steder, hændelsesforløb og personlige forhold, der kan sammenholdes med medieomtale eller andre åbne kilder og pege på de involverede personer. Tilsvarende problemstillinger kan opstå i sociale sager og på andre myndighedsområder.

---

[4] Lovudkastet, almindelige bemærkninger, pkt. 2.1.2, s. 16–17, og pkt. 2.2.2.3, s. 34–35. Udkastet etablerer ikke en generel hjemmel til videregivelse mellem myndigheder.

[5] Lovudkastet, almindelige bemærkninger, pkt. 5, s. 48–49, omtaler forventede effektiviseringsgevinster og implementeringsomkostninger. Det indeholder ikke en beregning af den second opinion-ordning, Edora foreslår.

[6] Datatilsynet, Hvad er personoplysninger? Se også GDPR, præambelbetragtning 26, om identifikation med midler, som med rimelighed kan forventes anvendt. Eksemplerne i teksten er illustrative.

Eksemplerne illustrerer genidentifikation. Profilering er et beslægtet, men andet spørgsmål: hvilke vurderinger eller forudsigelser der kan knyttes til personen. Begge risici bør indgå, men de bør ikke sammenblandes.

Det Europæiske Databeskyttelsesråd har desuden understreget, at AI-modeller trænet på personoplysninger ikke automatisk er anonyme. Der skal blandt andet vurderes risiko for, at personoplysninger kan udtrækkes eller fremkomme gennem forespørgsler.[7]

Edora anbefaler, at myndigheden dokumenterer risikoen ved kombination med andre datasæt, adgang til åbne kilder og udtræk fra selve modellen. Vurderingen bør dække træningsdata, model, søgeindeks, forespørgsler, svar og logning og opdateres ved væsentlige ændringer. En betegnelse som "anonymiseret" må ikke erstatte denne vurdering og betyder at umiddelbart harmløse data skal betragtes som GDPR-data.

3. Snowden og kabelsamarbejdet: Mere end udlevering efter anmodning

3.1. Løbende og automatiseret efterretningsindsamling

Risikoen for udenlandsk adgang må ikke reduceres til, om en leverandør kan modtage en enkeltstående anmodning om udlevering. Edward Snowdens afsløringer fra 2013 og den efterfølgende offentlige dokumentation viser, hvorfor efterretningsindsamling skal behandles som et selvstændigt spørgsmål.

Det amerikanske tilsynsorgan PCLOB beskrev i 2014 PRISM og Upstream under FISA Section 702. Indsamlingen var knyttet til udvalgte identifikatorer, eksempelvis e-mailadresser. Når en identifikator var aktiveret, kunne indsamlingen fortsætte løbende; der skulle ikke fremsættes en ny individuel udleveringsanmodning for hver meddelelse. Upstream omfattede teknisk filtrering af kommunikationsstrømme i netværksinfrastrukturen. Domstolskontrollen var ikke en individuel forhåndsgodkendelse af hvert overvågningsmål. Der var samtidig regler, måludvælgelse og pålæg til medvirkende leverandører.[8]

MUSCULAR-afsløringen beskrev NSA/GCHQ-aflytning af forbindelser mellem Google- og Yahoo-datacentre.[9]

Det relevante skel er derfor ikke "anmodning eller ingen risiko", men mellem forskellige adgangsformer: retlige udleveringspålæg, programbaseret indsamling, aflytning af kommunikationsforbindelser og anden skjult adgang.

3.2. Den danske kabeldimension

I 2021 beskrev DR, SVT og andre europæiske medier, med afsæt i oplysninger om den interne undersøgelse Operation Dunhammer, hvordan NSA ifølge deres kilder havde benyttet samarbejdet med Forsvarets Efterretningstjeneste om danske kommunikationskabler til at indsamle oplysninger om europæiske politikere, herunder Angela Merkel. Afdækningen beskrev blandt andet brug af telefonnumre som

[7] Det Europæiske Databeskyttelsesråd, Opinion 28/2024 om personoplysninger i AI-modeller, vedtaget 17. december 2024, resumé s. 2, om konkret vurdering af anonymitet og risiko for udtræk af personoplysninger.

[8] PCLOB, rapport om FISA Section 702, 2. juli 2014, s. 32–37 og 111–113. Se også PCLOB-rapporten fra 28. september 2023, s. 43, om programgodkendelse frem for individuel domstolsprøvelse af hvert mål. Beskrivelsen er historisk, ikke dokumentation for enhver leverandørs aktuelle systemer.

[9] The Washington Post, MUSCULAR-afsløringen, 30. oktober 2013.

søgekriterier i kommunikationsstrømme og systemet XKeyscore. Oplysningerne vedrørte et historisk forløb, blandt andet i 2012 og 2014.[10]

3.3. US CLOUD Act er en anden mekanisme

US CLOUD Act fra 2018 vedrører en anden adgangsvej. Omfattede leverandører under amerikansk jurisdiktion kan efter de relevante retlige procedurer pålægges at udlevere data under deres besiddelse, varetægt eller kontrol, selv om data opbevares uden for USA. Med eksemplerne ovenfor, hvor der er implementeret tekniske GOV-bagdøre og adgang til data er der en real risiko for at data automatisk udleveres til NSA.[11]

Edoras anbefaling er derfor, at risikoen vurderes ud fra **jurisdiktion, faktisk kontrol, adgangsveje, kommunikationsruter og tekniske beskyttelsesforanstaltninger** – ikke alene ud fra datacenterets adresse eller leverandørens kontraktuelle erklæringer.

4. Krav til suveræn og beredskabsegnet AI-drift

Med anvendelse AI kommer brugerne meget let til at fortælle modellerne ”hemmeligheder” som ikke i sit fragment er hemmelig, men ved at mange offentlige myndigheder benytter de samme få store AI-driftsoperatører bliver det meget let at sammenkøre af fragmenter på tværs at myndighederne til store dataset omkring den enkelte borger. Lovudkastet omfatter drift, men fastlægger ikke et generelt krav om **jurisdiktion**, dansk eller europæisk driftsplacering eller for den sags skyld spredning af AI-afvikling på tværs af flere forskellige driftsoperatører. Bemærkningerne overlader blandt andet tredjelandsoverførsler til de eksisterende databeskyttelsesregler. **Edora efterlyser derfor en udtrykkelig stillingtagen til placering og spredning af den underliggende infrastruktur og jurisdiktion i forbindelse med den nye hjemmel.**[12]

For følsomme og samfundskritiske anvendelser bør udgangspunktet være, at AI-modellerne faktisk afvikles på infrastruktur i Danmark eller EU/EØS med reel dansk eller europæisk juridisk og operationel kontrol. Det er ikke tilstrækkeligt, at kun lagringen sker i en europæisk region, hvis jurisdiktion, modelkørsel eller andre centrale funktioner ligger uden for det kontrollerede miljø.

Edora anbefaler fælles, bindende og risikobaserede minimumskrav med mulighed for skærpelse på særligt beskyttelseskrævende områder. Kravene bør omfatte tre sammenhængende forhold:

Data og modelkørsel. Kravene skal omfatte udvikling, træning og anvendelse, herunder selve afviklingen af forespørgsler, samt databaser, søgeindeks, sikkerhedskopier og logfiler. Eksterne tjenester, automatisk telemetri og supportkanaler skal indgå i kortlægningen. Betegnelsen “lokal AI” bør ikke kunne bruges om en løsning, der i praksis videresender de beskyttede oplysninger til en ekstern modeltjeneste.

[10] SVT, fælles undersøgelse med blandt andre DR, 30. maj 2021, opdateret 31. maj 2021. Det er journalistisk afdækning af et hemmeligt forløb. Til afgrænsning: Forsvarsministeriets meddelelse, 13. december 2021, oplyser, at FE-kommissionen inden for sit undersøgelsesområde ikke fandt grundlag for kritik af FE eller de undersøgte medarbejdere.

[11] U.S. Department of Justice, The Purpose and Impact of the CLOUD Act – FAQs, spørgsmål 17–24, navnlig 20–22, om udleveringskrav, jurisdiktion og data under leverandørens besiddelse, varetægt eller kontrol.

[12] Lovudkastet, § 2, nr. 5–6, og almindelige bemærkninger, pkt. 1.1, s. 7, pkt. 2.2.2.1, s. 29, og pkt. 5, s. 50. GDPR, navnlig artikel 24, 25, 28, 32, 35 og kapitel V, gælder fortsat.

Jurisdiktion, adgang og nøglekontrol. Myndigheden skal kunne dokumentere leverandørkæden, kontrol fra eventuelle moderselskaber, administrative adgange og hvem der kan disponere over krypteringsnøgler. Der bør stilles krav til begrænset, godkendt og sporbar adgang samt uafhængig kontrol. Kryptering bør ikke alene vurderes under lagring og transport, men også i forhold til, hvem der kan få adgang til læsbare oplysninger under behandlingen.

Beredskab og mulighed for at skifte leverandør. Myndigheden skal have testede planer for genetablering, uafhængige sikkerhedskopier og en realistisk mulighed for at videreføre eller erstatte løsningen, hvis en leverandør, netværksforbindelse eller central login- og licenstjeneste bortfalder. Kritiske opgaver skal kunne håndteres via et alternativt driftsmiljø eller en forsvarlig manuel arbejdsgang. Eksport af data alene er ikke tilstrækkelig, hvis modellen og de nødvendige afhængigheder ikke kan genetableres.

Kravene skal være proportionale med opgaven og udformes i overensstemmelse med EU-retten. Et eventuelt krav om Danmark frem for et andet EU/EØS-land skal begrundes særskilt i konkrete sikkerheds- eller beredskabsbehov. Fravigelser af et udgangspunkt om europæisk drift bør kræve dokumenteret nødvendighed, beskyttelsesforanstaltninger og ansvarlig godkendelse. En fravigelse kan ikke tilsidesætte GDPR eller anden gældende ret.

5. Det offentlige som strategisk og klog indkøber

5.1. Indkøb former fremtidens kapacitet

Edora mener, at det offentlige bør bruge sin efterspørgsel til at understøtte opbygning af dansk og europæisk AI-, cloud- og datacenterkapacitet. Offentlige indkøb er ikke kun løbende driftsudgifter; de er også med til at forme, hvor investeringer, kompetencer og teknologisk handlefrihed opbygges.

Dette bør omsættes til saglige krav om jurisdiktion, sikkerhed, suverænitet, interoperabilitet, dokumentation, exitmuligheder og samlet økonomi.

5.2. Kontrol er vigtigere end at være først

Det offentlige bør ikke gøre adgang til den allernyeste AI-model til et mål i sig selv. På områder med myndighedsudøvelse og følsomme oplysninger kan det være ansvarligt at anvende en tilstrækkeligt god, afprøvet model, selv om den eksempelvis er tre til seks måneder bag den nyeste lancering, når det giver bedre kontrol, sikkerhed og driftsuafhængighed. Edora mener at modellerne skal kunne installeres lokalt og være OpenSource, så det er muligt for tredje mand at verificere modellerne.

Det er ikke et forslag om en fast ventetid eller om at acceptere utilstrækkelig kvalitet. Det er et forslag om at vægte dokumenteret egnethed og langsigtet handlefrihed højere end markedsføring af den nyeste model. Internationale modeller kan godt indgå, når licensvilkår og teknisk udformning gør det muligt at afvikle dem i det ønskede kontrollerede miljø. Modellens oprindelse og dens konkrete driftsform skal vurderes hver for sig.

6. Edoras samlede anbefaling

Edora anbefaler, at lovforslaget og den tilhørende implementering styrkes på følgende tre punkter:

For det første: En udtrykkelig, gebyrfri ret til en uafhængig menneskelig second opinion, hvor AI-vurderinger ikke overføres til eller anvendes af den nye vurderingsfunktion. Tværkommunal vurdering og en særskilt funktion i Ankestyrelsen bør undersøges som konkrete modeller, med klar hjemmel og uden svækkelse af de eksisterende klagerettigheder.

For det andet: Fælles, bindende minimumskrav til risikovurdering, faktisk driftsplacering, jurisdiktion, adgang, genidentifikation og beredskab. Vurderingen skal omfatte både retlige udleveringspålæg og risikoen for løbende, automatiseret efterretningsindsamling.

For det tredje: En offentlig indkøbspraksis, der inden for udbudsreglerne understøtter dansk og europæisk kapacitet, undgår uhensigtsmæssig leverandørafhængighed og prioriterer kvalitet, sikkerhed og kontrol frem for alene den nyeste model.

Vi bør ikke vælge mellem effektiv offentlig AI og borgernes retssikkerhed. Vi bør indrette lovgivningen og infrastrukturen, så vi kan opnå begge dele.

Med venlig hilsen

Group CEO
Mads Hedegaard
tlf. 21260550
mail mhe@edora.dk
Edora Group

EG Danmark A/S

Hedeager 44
8200 Aarhus N

Til Digitaliseringsstyrelsen
att. Jonathan Meijer og Lea Marie Omdahl

12. oktober 2026

Sendt per email til:
jonmei@digst.dk
emimol@digst.dk
leaomd@digst.dk
kahevi@digst.dk

Høringssvar fra EG vedr. forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven), jf. høringsbrev af 14. september 2026

1. Indledning

EG Danmark A/S (EG) er en dansk softwarevirksomhed, der leverer IT-løsninger, herunder løsninger med kunstig intelligens (AI), til offentlige myndigheder. I EG's AI-produkter er de offentlige kunder typisk dataansvarlige, og EG optræder som databehandler. EG er ikke opført på høringslisten, men har som leverandør af AI-løsninger til offentlige kunder en direkte interesse i lovforslaget.

EG støtter lovforslagets formål om at skabe et klarere og mere ensartet retsgrundlag for offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger. Efter EG's erfaring fra dialogen med kunder har usikkerhed om retsgrundlaget været en reel barriere for, at myndigheder tager AI i brug. EG er som medlem af Dansk Industri og IT-Branchen bekendt med branchens bemærkninger og ønsker med dette høringssvar at supplere med tre forhold set fra en leverandørs perspektiv, som efter EG's opfattelse har særlig betydning for, hvordan loven kan anvendes i praksis, når myndighederne udvikler og anvender AI-systemer i samarbejde med leverandører:

- leverandørens rolle ved udvikling og træning af AI-systemer (afsnit 2),
- kravene til menneskelig involvering ved beslutningsstøtte (afsnit 3), og
- betydningen af sletning af træningsdata for allerede trænede modeller (afsnit 4).

2. Udvikling og træning hos leverandøren som databehandler

Det fremgår af lovforslagets almindelige bemærkninger:

> *"Den foreslåede ordning vil desuden medføre, at personoplysninger vil kunne anvendes både til udvikling og til anvendelse af et AI-system. Dermed har offentlige myndigheder og organer mulighed for selv at udvikle eller få udviklet*

> *specialiserede AI-systemer, der er trænet på konkret og relevant træningsdata, herunder personoplysninger i myndighedens historiske og lukkede sager."*
> (lovforslaget, s. 29)

EG forstår formuleringen "selv at udvikle eller få udviklet" sådan, at hjemlen også omfatter de tilfælde, hvor udviklingen udføres af en leverandør på myndighedens vegne. Dette fremgår dog ikke udtrykkeligt af hverken lovteksten eller bemærkningerne, og databehandlerrollen er ikke omtalt i lovforslaget.

I praksis vil en væsentlig del af myndighedernes udvikling, træning, afprøvning, validering og gentræning af AI-systemer, jf. definitionen af "udvikling" i § 2, nr. 5, blive udført af leverandører i leverandørens tekniske miljø.

Af hensyn til retssikkerheden for både myndigheder, leverandører og borgere foreslår EG, at det i bemærkningerne til § 3 præciseres:

a) at udvikling og anvendelse efter § 3 omfatter behandling, som en databehandler udfører på vegne af og efter instruks fra den dataansvarlige myndighed eller det dataansvarlige organ, jf. databeskyttelsesforordningens artikel 28,
b) at dette også omfatter træning, gentræning og videreudvikling hos leverandøren på grundlag af personoplysninger, herunder personoplysninger i myndighedens historiske og lukkede sager, og
c) hvilke rammer, der gælder, når en leverandør udvikler fælles modeller eller foretager finjustering på tværs af flere myndigheder eller organer.

Punkt c) skal ses i lyset af, at lovforslaget efter bemærkningerne (s. 16 og s. 71) ikke giver hjemmel til videregivelse af personoplysninger mellem myndigheder og organer. Samtidig lægger bemærkningerne (s. 16-17) til grund, at fuldt anonymiserede oplysninger ikke er omfattet af lovforslaget, og at myndighederne selv skal vurdere, om et AI-system i sig selv udgør personoplysninger. EG opfordrer til, at bemærkningerne beskriver, hvordan disse forhold spiller sammen, når en leverandør på vegne af flere myndigheder udvikler eller forbedrer et AI-system, så det står klart, under hvilke betingelser en model, der er udviklet eller finjusteret på én myndigheds data, kan anvendes eller videreudvikles til gavn for andre myndigheder.

EG ønsker ikke at ændre ansvarsfordelingen mellem myndigheden som dataansvarlig og leverandøren som databehandler. Formålet er alene at sikre, at den hjemmel, som lovforslaget etablerer, også i praksis kan udnyttes i det samarbejde med leverandører, som størstedelen af myndighedernes udvikling af AI-systemer vil foregå i.

3. Menneskelig involvering ved beslutningsstøtte

Det fremgår af bemærkningerne (s. 65), at tilsynet med AI-systemets output skal være meningsfuldt og ikke alene udgøre en tom gestus, og at evalueringen bør foretages af en person med de fornødne kompetencer og mulighed for selv at foretage vurderingen og ændre forslaget. Samtidig forventes det, at fremtidig praksis vil præcisere, hvilken grad af menneskelig involvering der kræves, for at anvendelsen kan anses som beslutningsstøtte og ikke som en fuldautomatiseret afgørelse efter databeskyttelsesforordningens artikel 22.

EG er enig i udgangspunktet. Afgrænsningen er imidlertid afgørende for, om en given løsning falder inden for lovens anvendelsesområde, og den bør derfor ikke alene overlades til fremtidig praksis. For leverandører kan det være et centralt designparameter, hvordan en sagsbehandler involveres i og kan påvirke AI-systemets output. Uden en nærmere konkretisering vil myndigheder og leverandører have vanskeligt ved at vurdere, om en løsning lever op til kravene, allerede når løsningen designes.

EG ser meget positivt på, at Digitaliseringsstyrelsen i høringsbrevet oplyser at prioritere vejledning. EG foreslår, at der udarbejdes vejledning, som:

a) angiver typetilfælde for anvendelse af beslutningsstøtte, f.eks. udkast til afgørelser, prioritering af sager og risikoscorer,
b) for hvert typetilfælde beskriver, hvad der kendetegner meningsfuld menneskelig involvering, og
c) giver eksempler på tekniske og organisatoriske foranstaltninger, som kan understøtte meningsfuld involvering, f.eks. logning, forklaringsfunktioner samt mulighed for at afvige fra AI-systemets forslag og dokumentere afvigelsen.

EG bidrager gerne med erfaringer fra udviklingen af konkrete løsninger i forbindelse med udarbejdelsen af vejledningen.

4. Sletning af træningsdata og allerede trænede modeller

Det fremgår af bemærkningerne (s. 71), at lovforslaget alene giver mulighed for at viderebehandle personoplysninger, som myndigheden har lovlig adkomst til at opbevare, og at oplysninger, som ikke længere er nødvendige at behandle for opgavevaretagelsen, ikke lovligt kan anvendes til udvikling af et AI-system. EG er enig heri.

Lovforslaget tager derimod ikke stilling til, hvad der gælder for et AI-system, som lovligt er trænet på oplysninger, der efterfølgende skal slettes. Bemærkningerne anerkender (s. 40 og s. 77), at det ikke altid vil være muligt at udskille de registreredes personoplysninger fra modelparametrene i et AI-system. Da ”udvikling” efter § 2, nr. 5, også omfatter gentræning, er der efter EG's opfattelse behov for at afklare, om sletning af træningsdata udløser et krav om, at modellen gentrænes.

EG foreslår, at det i bemærkningerne præciseres:

a) at træning, som var lovlig på tidspunktet for træningen, ikke bliver ulovlig, fordi de underliggende træningsdata senere slettes i overensstemmelse med gældende regler,
b) at sletning af træningsdata derfor ikke i sig selv medfører en pligt til at gentræne eller udfase en allerede trænet model, og
c) at dette forudsætter, at modellen ikke indeholder personoplysninger om de registrerede, hvis oplysninger skal slettes, i en form, hvor oplysningerne kan henføres til den enkelte registrerede.

En sådan præcisering vil sikre, at borgernes ret til sletning respekteres, uden at myndighederne pålægges at gentage omkostningstunge træningsforløb i situationer, hvor modellen ikke indeholder direkte henførbare personoplysninger. EG opfordrer samtidig til, at vejledningen

beskriver, hvordan myndighederne kan vurdere og dokumentere, at en model ikke indeholder direkte henførbare personoplysninger, og hvilke foranstaltninger der forventes i de tilfælde, hvor det ikke kan udelukkes.

5. Afslutning

EG står gerne til rådighed for en uddybning af bemærkningerne og deltager gerne i den videre dialog om vejledning og implementering af loven.

Med venlig hilsen

Sune Albert
General Counsel, Vice President, Group Legal & Compliance, EG Danmark A/S

Digitaliseringsstyrelsen

Høring: Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

F&P har ikke konkrete bemærkninger til forslaget, men vil dog påpege, at lovforslaget fremhæver en mere generel udfordring for innovation med AI.

Hvis offentlige myndigheder med adgang til hjemler efter artikel 6, stk. 1, litra e, oplever behov for yderligere lovgivningsmæssig afklaring for at kunne udvikle og anvende AI-systemer, kan tilsvarende udfordringer forventes at gøre sig gældende med afsæt i de hjemler, der er tilgængelige for den private sektor.

Lovforslaget kan derfor ses som et udtryk for, at spørgsmålet om databeskyttelsesretlige rammer for AI er en generel udfordring med betydning for innovation og digital udvikling i erhvervslivet.

Hvis man fra dansk side ser generelle udfordringer og barrierer for innovation med AI, vil det være relevant at fremhæve disse i de danske indspil til den igangværende proces på den Digitale Omnibus samt det kommende digitale Fitness Check.
Forslag der fra Kommissionens side netop har til formål at reducere barrierne for AI og innovation, når det er muligt uden at kompromittere den grundlæggende beskyttelse.

Med venlig hilsen
Jakob Holm
Chefkonsulent, Digitaliseringspolitik
jho@fogp.dk | +45 41 91 91 76

12.10.2026

F&P
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
fp@fogp.dk
www.fogp.dk
CVR 11 62 81 84

Jakob Holm
Chefkonsulent
Dir. 41919176
jho@fogp.dk

Sagsnr. GES-2019-00312
DokID 560019

Brancheorganisation
for forsikringsselskaber
og pensionskasser

FAXE KOMMUNE

Stab for Økonomi & Teknologi

Postadresse:
Frederiksgade 9
4690 Haslev
Telefon 56203000

Kontoradresse:
Digitalisering
Frederiksgade 9
4690 Haslev

www.faxekommune.dk

Dato: 30. september 2026

Sagsnummer:
85.10.00-G01-2-26

Høringssvar vedr. forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Du bør bruge Digital Post eller sende/aflevere et fysisk brev, hvis du vil skrive til os. Sådan beskytter du bedst dine oplysninger.

Dine personoplysninger passer vi godt på! Du kan læse om, hvordan vi behandler dine oplysninger, og hvilke rettigheder du har på www.faxekommune.dk.

Hermed fremsender Faxe Kommune høringssvar vedr. forslag til AI-hjemmelsloven.

Klare grænser for beslutningsstøtte

Grænsen mellem administrativ understøttelse, beslutningsstøtte og automatiseret beslutningstagning fremstår ikke operationelt anvendelig i lovforslaget.

Faxe Kommune skal hermed efterspørge, at hjemmelsloven snarest mulig ledsages af en praksisnær vejledning med kommunale eksempler. Det kan være systemer, der opsummerer en borgersag, udarbejder et baggrundsnotat, foreslår næste skridt i et forløb eller skriver et udkast til en afgørelse. Vejledningen bør gøre det muligt at vurdere kravene allerede ved anskaffelse, risikovurdering og implementering.

Det bør i denne vejledning præciseres, hvorvidt det fx er tilstrækkeligt, at en medarbejder formelt godkender et resultat samt at der bør være en reel faglig stillingtagen til AI-systemets forslag.

Afgrænsningen af behandlingsgrundlaget

Det bør præciseres, hvilken praktisk betydning lovforslagets afgrænsning til databeskyttelsesforordningens artikel 6, stk. 1, litra e, får på kommunale myndighedsområder, hvor behandlingen følger af konkrete lovbestemte forpligtelser. Dertil fremstår det ikke tydeligt, hvorledes afgrænsningen foretages fsva. oplysninger, der behandles med øvrig hjemmel, herunder med hjemmel i databeskyttelsesforordningens artikel 6, stk. i litra c samt artikel 9. Det kan hertil bemærkes, at oplysninger jævnligt behandles med

dobbelthjemmel, eller der fremkommer oplysninger, der reelt behandles med forskellig hjemmel i ustrukturerede data – fx i AI-løsninger der behandler data fra en optaget borgersamtale. Det er derfor vigtigt, at der i selve loven tages højde for, at der ikke kan opstå tvivl om, i hvilket omfang loven tilsidesætter andre regler.

Sammenhæng mellem sektorregler
Kommunale arbejdsgange går ofte på tværs af ressortområder. Det gælder blandt andet på beskæftigelsesområdet, hvor helbredsoplysninger og oplysninger om borgerens sociale situation kan indgå i den samme sag. Faxe Kommune skal opfordre til en koordineret udmøntning af reglerne om passende og specifikke foranstaltninger jf. lovforslagets § 3 stk. 2 samt § 4, stk. 1. Der kunne med fordel udpeges en koordinerende minister.

Behovet for koordinering af sektorregler gør sig også gældende på hjemmelspørgsmål. Her bør det sikres, at eventuelle sektorspecifikke regler, herunder hjemler, bør koordineres med henblik på at sikre, at området ikke bliver unødigt komplekst at fortolke og forvalte.

Faxe Kommune skal opfordre til, at der i lovbemærkningerne præciseres om der med ordvalget i § 3, stk. 1 alene er tale om, at oplysninger som kommunen i forvejen behandler kan anvendes til fx udvikling af AI-løsninger. Såfremt kommunerne ikke kan anvende oplysninger, som fx oprindeligt er behandlet af andre kommuner (eller af andre myndighedsområder indenfor egen kommune), kan der opstå praktiske udfordringer i kommunernes udviklings- og driftsfællesskaber.

Fælles begreber, dokumentationsstandarder og minimumskrav bør kunne suppleres med sektorspecifikke krav, når det er nødvendigt. Meget forskellige regelsæt vil gøre anvendelsen unødigt kompleks.
Det bør også sikres, at der ikke kan opstå tvivl om, hvilke regelsæt der skal betragtes som lex specialis.

Datakvalitet og menneskeligt ansvar
Anvendelse af AI til beslutningsstøtte og profilering kræver særlig opmærksomhed på datakvalitet og risikoen for systematiske skævheder. Historiske sager kan afspejle tidligere praksis og indeholde fejl eller skævheder, som ikke bør videreføres i nye vurderinger.
Faxe Kommune skal hermed efterspørge tydelige og proportionale krav til løbende validering, håndtering af fejl og dokumentation af menneskelig kontrol. Det skal være klart, hvordan medarbejderen forventes at efterprøve systemets output, og hvordan dette kan dokumenteres i praksis. Kravene bør afspejle anvendelsens betydning for borgeren. Et værktøj til referatskrivning og et system, der anbefaler indsatser eller bidrager til en afgørelse, stiller forskellige krav til faglig kontrol.

Borgernes rettigheder og gennemsigtighed
Borgernes tillid afhænger af, at de kan forstå, hvordan AI indgår i behandlingen af deres oplysninger, og hvordan de kan få fejl rettet og myndighedens behandling efterprøvet. Herunder kan det med fordel præciseres, hvad rammerne er for viderebehandling af personoplysninger til formål forbundet med udvikling og træning af AI-løsninger samt hvordan registreredes rettigheder generelt imødegås i forbindelse hermed.

Faxe Kommune skal hertil understrege, at eventuelle begrænsninger af borgernes rettigheder skal være konkrete, nødvendige og klart afgrænsede.

Anvendelsen af AI bør ikke i sig selv medføre mindre gennemsigtighed. Der er samtidig behov for praktisk vejledning om, hvordan kommunerne opfylder fx oplysningspligten på en forståelig måde.

Implementering og økonomi
Et tydeligere hjemmelsgrundlag er væsentligt, men den praktiske anvendelse kræver også ressourcer til indkøb, implementering, oplæring, kvalitetskontrol og vedligeholdelse samt efterlevelse af eksisterende lovgivning. Gevinsterne afhænger af den konkrete opgave, teknologi og organisation og kan ikke forudsættes at opstå automatisk.

Faxe Kommune skal opfordre til, at hjemmelslovgivningen suppleres af fælles vejledninger, skabeloner, metoder til risikovurdering og fortolkningsbidrag, som kan genbruges på tværs af kommuner. Den generelle hjemmel får størst praktisk værdi, hvis den også mindsker behovet for, at hver kommune foretager de samme juridiske og organisatoriske afklaringer.

Med venlig hilsen

Ann Kamgård Haugaard
Chefkonsulent

Til: leaomd@digst.dk, emimol@digst.dk, kahevi@digst.dk, jonmei@digst.dk
Cc: CTN@FTNET.DK (Christina Thorup Sand (FT)), Ministerbetjening@FTNET.DK (Ministerbetjening (FT))
Fra: Rasmus Engelbrecht (RAEN@FTNET.DK)
Titel: Høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger
Sendt: 09-10-2026 12:47
Bilag: image001.png; image002.png;

Finanstilsynet takker for muligheden for at afgive høringssvar til lovforslaget.

Finanstilsynet finder det navnlig positivt, at lovforslaget indeholder en fortolkning af begrebet "beslutningsstøtte", jf. side 68. Begrebet har hidtil givet anledning til afgrænsningsmæssige vanskeligheder. Med bemærkningerne til § 2, nr. 4, opstilles der fire kumulative betingelser for, hvornår et system kan anses for at udgøre beslutningsstøtte og dermed falde uden for forbuddet i databeskyttelsesforordningens artikel 22, stk. 1.

Denne præcisering bidrager efter Finanstilsynets vurdering til at skabe større klarhed om rammerne for udvikling og anvendelse af automatiserede systemer.

Finanstilsynet vurderer i øvrigt, at lovforslaget adresserer de væsentligste forhold på området, herunder forhold som allerede må anses for afklaret enten i litteraturen eller gennem retspraksis.

Finanstilsynet har ikke yderligere bemærkninger.

Med venlig hilsen
Rasmus Engelbrecht
Fuldmægtig, cand.merc.jur.
Juridisk kontor

FINANSTILSYNET
Strandgade 29
1401 København K
Tlf.: +45 33 55 82 82
Direkte tlf.: +45 29 83 19 78
Mail: RAEN@ftnet.dk
www.finanstilsynet.dk

Finanstilsynet er ansvarlig for behandlingen af de personoplysninger, vi modtager om dig. Du kan læse mere om, hvordan vi behandler dine personoplysninger på vores hjemmeside https://www.finanstilsynet.dk/organisationen/privatlivspolitik
Finanstilsynet gør opmærksom på, at denne e-mail og eventuelle vedhæftede filer er fortrolige. Hvis du har modtaget denne mail ved en fejl, bedes du straks oplyse Finanstilsynet herom ved at besvare denne e-mail og derefter slette e-mailen. Vi gør opmærksom på, at hvis du har modtaget denne e-mail ved en fejl, kan enhver form for kopiering, offentliggørelse eller distribution af denne e-mail være ulovlig.

Fra: Jonathan Kirkegaard Meijer <jonmei@digst.dk>
Sendt: 14. september 2026 10:41
Emne: Høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Kære høringspart

Digitaliseringsstyrelsen anmoder hermed om eventuelle bemærkninger til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Eventuelle høringssvar bedes fremsendt via e-mail
til jonmei@digst.dk, kahevi@digst.dk, emimol@digst.dk og leaomd@digst.dk senest kl. 12:00 den 12. oktober 2026.

Høringsmaterialet kan også ses på Høringsportalen via følgende link: https://hoeringsportalen.dk/Hearing/Details/71477 hvor modtagne høringssvar også vil blive gjort tilgængelige.

Med venlig hilsen

Digitaliserings-
styrelsen

Jonathan Meijer

Fuldmægtig
Kontor for AI, analyse og inklusion

T 2485 9061
E jonmei@digst.dk

_____

www.digst.dk

Du bedes venligst være opmærksom på, at Digitaliseringsstyrelsen ved modtagelsen af din meddelelse behandler de personoplysninger om dig, der fremgår af beskeden. Dette sker som led i Digitaliseringsstyrelsens myndighedsudøvelse. Du kan læse mere om, hvordan Digitaliseringsstyrelsen behandler dine personoplysninger, og hvilke rettigheder du har som registreret mv., i styrelsens privatlivspolitik https://digst.dk/om-os/privatlivspolitik/

FORBRUGERRÅDET tænk

12. oktober 2026

Høringssvar til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Forbrugerrådet Tænk takker for at blive inddraget i høringen af lovudkastet om udvikling og anvendelse af AI-systemer i den offentlige forvaltning. Forbrugerrådet Tænk er enige i intentionen om at skabe klar hjemmel til udvikling og anvendelse af allerede indsamlede personoplysninger til udvikling og anvendelse af AI-systemer i det offentlige. Efter Forbrugerrådet Tænks vurdering er der dog flere forhold, som påkalder sig særlig opmærksomhed:

Bemærkning om hvad loven tillader AI-systemer at blive brugt til

Forbrugerrådet Tænk finder det positivt at der i forslaget fremgår flere eksempler på arbejdsgange, der omfattes af beslutningsstøtte. Lige så støtter vi op på den nære iagttagelse af ikke at tillade behandlinger som vil bryde med databeskyttelsesforordningens artikel 22 om fuldautomatiserede afgørelser.

Trods tilføjelsen af flere konkrete eksempler erkender forslaget at de ikke kan komme det nærmere i forslagets udkast, og at det må "*forventes, at fremtidig praksis vil bidrage til at præcisere, hvilken grad af menneskelig involvering der kræves for, at anvendelsen af et AI-system kan anses som beslutningsstøtte og ikke fuldautomatiserede*"[1].

Selvom Forbrugerrådet Tænk kan tilslutte sig lovudkastets sigte om at skabe et samlet retsgrundlag for AI-løsninger i det offentlige og i øvrigt ikke ændrer ved Forvaltningslovens bestemmelser om korrekt og oplyst sagsbehandling, bør en generel AI-hjemmel – i lyset af Datatilsynets bemærkning - adressere, at den offentlige forvaltnings funktionsmåde, dens afgørelser og relation til borgerne vil blive påvirket af en øget AI-anvendelse med egne trænede modeller.

Som det også bemærkes i udkastets omtale af AI-løsninger til beslutningsunderstøttelse, har Datatilsynet i tilknytning til en konkret sag bemærket at *"… Brug af AI-løsninger medfører, at AI løsninger kan lære, finde sammenhænge og gennemføre sandsynlighedsanalyser og drage konklusioner langt ud over det, som en fysisk sagsbehandler vil være i stand til".*[2]

Det er således ikke tilstrækkeligt, at de persondataretlige problemstillinger adresseres i udkastet. En kommende lov bør mere eksplicit forholde til, hvor man skal sætte grænsen mellem 'beslutnings-understøttelse' og egentlig sagsbehandling, der har konsekvenser for borgeren (jf. også, at et AI-system efter lovudkastet vil kunne anvendes til evaluering af bestemte personlige forhold vedrørende en borger).

Det bør i den forbindelse overvejes at stille som krav, at den offentlige forvaltning ved meddelelse til borgeren om en afgørelse, der er baseret på AI-anvendelse til beslutningsunderstøttelse og evaluering, bliver forpligtet til at oplyse om 1. AI-systemets beslutningsunderstøttende anbefaling/ evaluering i den givne sag 2. Forvaltningens overvejelser på baggrund af anbefalingen / evalueringen 3. Forvaltningens begrundede afgørelse efter de almindelige forvaltningsretlige principper.

[1] Forslagets bemærkninger side 65
[2] Forslagets bemærkninger side 22

Bemærkninger om tredjelandsoverførsler og digital suverænitet

Det fremgår af udkastet, at loven ikke adresserer problemstillinger, der er relateret til tredjelandsoverførsler.[3]

I lyset af debatten om digital uafhængighed (og den generelle debat om cybersikkerhed, udviklingen i risikobilledet, digitale rettigheder og digital innovation i Europa) bør lovforslaget netop adressere tredjelandsproblematikken. Det kan ske ved, at de AI-modeller, som loven giver danske offentlige myndigheder øgede mulighed for at udvikle, som udgangspunkt alene trænes på grundlag af AI-træningsmetoder, der ikke samtidig medfører dataoverførsel mellem den specialiserede danske model og eventuelt store træningsmodeller, som måtte blive anvendt som træningsfundament.

Det er muligt at visse nye offentlige AI-modeller kun kan udvikles ved at den omtalte dataoverførsel finder sted. Derfor bør de under alle omstændigheder stilles som krav, at offentlige instanser (jf. lovforslagets definition) i videst mulige omfang anvender privatlivsfremmende teknologier i udvikling og den løbende vedligeholdelse af AI-modellerne.

Bemærkninger om indskrænkelsen af de registreredes rettigheder

Forslaget finder det relevant at indskrænke flere af de registreredes rettigheder, med henvisning til de teknologiske begrænsninger der ofte vil være til stede når man udvikler og anvender AI systemer, idet ”*AI-systemer er ofte kendetegnet ved komplekse datastrukturer, hvor oplysninger fra mange registrerede potentielt vil indgå i træningsdata*”.

Forbrugerrådet Tænk anerkender, at borgernes rettigheder for personoplysninger, der indgår i træningen af en AI-model, kun meget vanskeligt og omkostningsfuldt kan imødekommes. Dog har vi svært ved at se den samme indskrænkning godtgjort, når det kommer til anvendelsen af AI-systemer.

Det er derfor afgørende, at den offentlige forvaltning er forpligtet til gennemsigtighed, hvad angår AI-modellernes funktionsmåde, deres anvendelsesformål og -afgrænsning, hvilke typer persondata, der er anvendt i udviklingen samt ikke mindst, hvordan den enkelte borgers persondata fortsat vil være beskyttet mod datalæk, misbrug og profilering. Ligeledes er det vigtigt, at den offentlige forvaltning gennemfører risikovurderinger og evt. konsekvensanalyser, hvor de registreredes risiko er i fokus.

Forbrugerrådet Tænk skal i tilknytning hertil og i lyset af EU Domstolens afgørelse C-175/20[4] bemærke, at loven giver en meget bred hjemmel til en meget bred gruppe af aktører, som omfattet af forvaltningsloven.[5] Forbrugerrådet Tænk er ikke overbevist om at en så bred hjemmel udgør ”enkle og klare regler”.[6]

[3] Forslagets bemærkninger side 7
[4] Se fx https://www.juridicainternational.eu/article_full.php?uri=2024_33_data-driven_public_administration_and_the_gdpr_seeing_the_court_of_justice_s_judgement_in_ca
[5] Forslagets bemærkninger side 12
[6] Forslagets bemærkninger side 49

For uddybende bemærkninger eller spørgsmål hertil, bedes I kontakte:

Uffe Rabe Krag

POLITISK CHEF

T +45 4188 1610
W taenk.dk
Forbrugerrådet Tænk
Ryesgade 3A, 2. th. |
2200 Kbh. N

Ida Nynne Daarbak Reislev
SENIORJURIST

M +45 5081 0031
W taenk.dk
Forbrugerrådet Tænk
Ryesgade 3A, 2. th. |
2200 Kbh. N

Peter Grønlund Holm

FORBRUGERPOLITISK RÅDGIVER
M +45 4188 1608
W taenk.dk
Forbrugerrådet Tænk
Ryesgade 3A, 2. th. |
2200 Kbh. N

DANSKE REVISORER FSR

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Att.: Fuldmægtig Jonathan Meijer og fuldmægtig Katerina Helena Vinther
Pr. e-mail: jonmei@digst.dk; emimol@digst.dk; leaomd@digst.dk; kahevi@digst.dk

12. oktober 2026

FSR – danske revisorer

Børsgade 4, 4. sal
DK - 1215 København K

Telefon +45 7225 5703
fsr@fsr.dk
www.fsr.dk

CVR. 55 09 72 16
Danske Bank
Reg. 9541
Konto nr. 2500102295

FSR Danske Revisorers høringssvar vedrørende fornyet høring over forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

FSR Danske Revisorer takker for muligheden for at afgive bemærkninger til det reviderede forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger. Vi afgav høringssvar til det oprindelige lovforslag den 2. marts 2026. Ændringerne i det reviderede forslag ændrer ikke ved vores bemærkninger, som derfor fastholdes i deres helhed nedenfor (afsnit 1 til 8). I afsnit 9 har vi tilføjet bemærkninger til de ændringer, der er foretaget.

FSR Danske Revisorer repræsenterer godkendte revisorer (statsautoriserede og registrerede revisorer) i Danmark. Vores medlemmer fører i dag uafhængigt tilsyn og afgiver erklæringer om både offentlige og private organisationers efterlevelse af databeskyttelsesforordningen (GDPR), generelle it-kontroller (herunder ISAE 3402 og ISAE 3000), cybersikkerhed og øvrige kontrolmiljøer relateret til digital behandling af oplysninger – herunder også kontroller knyttet til anvendelse af AI-teknologier.

Revisorstanden fungerer således allerede i dag som en central og systembærende kontrolaktør i relation til digitale risici, databeskyttelse og teknologibaseret governance – både i den private og den offentlige sektor.

Vi støtter intentionen om at skabe et generelt retsgrundlag for offentlig anvendelse af AI. Samtidig finder vi, at lovforslaget efterlader væsentlige spørgsmål om governance, kontrol og efterprøvelighed ubesvarede.

1. Supplerende retsgrundlag – manglende præcisering af kontrolramme

Lovforslaget etablerer det nationale supplerende retsgrundlag, som kræves efter GDPR artikel 6, stk. 1, litra e, jf. artikel 6, stk. 3.

Det fremgår imidlertid ikke af lovforslaget:

- Hvilke konkrete kontrolkrav der skal gælde ved anvendelse af hjemlen
- Hvordan proportionalitetsvurderingen skal dokumenteres
- Hvordan overholdelse af garantier skal kunne efterprøves.

Efter EU-Domstolens praksis skal nationale hjemler være klare og præcise og indeholde tilstrækkelige garantier mod misbrug.

Når lovforslaget indfører en bred og teknologineutral adgang, uden samtidig at fastsætte strukturerede krav til dokumentation og kontrol, opstår der en asymmetri mellem adgang og kontrol.

Vi finder derfor, at der bør præciseres krav om dokumenteret governance og kontrolstruktur som forudsætning for anvendelse af hjemlen.

2. Accountability – manglende krav om dokumenteret intern kontrol

GDPR artikel 5, stk. 2, og artikel 24 pålægger den dataansvarlige at kunne påvise overholdelse.

Lovforslaget henviser generelt til fortsat overholdelse af GDPR, men fastsætter ikke:

- Krav om formaliserede AI-governance-strukturer
- Krav om dokumenteret risikostyringsramme
- Krav om periodisk intern eller ekstern gennemgang.

AI-systemer – særligt ved træning og løbende videreudvikling – indebærer betydelig kompleksitet og risiko for systematiske fejl eller bias.

FSR Danske Revisorer finder derfor, at lovgivningen bør suppleres med eksplicit krav om dokumenteret kontrolmiljø, således at accountability-princippet i praksis kan efterleves.

3. Menneskeligt tilsyn – manglende operationalisering

Lovforslaget forudsætter, at AI alene anvendes som beslutningsstøtte og ikke til automatiserede afgørelser (jf. GDPR artikel 22).

Der fremgår imidlertid ikke:

- Hvordan menneskeligt tilsyn konkret skal udøves
- Hvordan kompetencekrav til sagsbehandlere skal dokumenteres
- Hvordan afhængighed af systemets output skal kontrolleres.

AI-forordningens artikel 14 kræver, at højrisiko-AI er underlagt effektivt menneskeligt tilsyn.

Uden nærmere operationalisering risikerer kravet om menneskelig involvering at blive formelt frem for reelt.

Vi finder derfor, at der bør indarbejdes krav om dokumentation af menneskeligt tilsyn og kontrol.

4. Særlige kategorier af oplysninger – manglende eksplicitte garantier

Lovforslaget forudsætter korrekt dobbelt hjemmelskrav efter GDPR artikel 6 og artikel 9.

Det fremgår imidlertid ikke:

- Hvilke minimumsgarantier der skal gælde ved behandling af følsomme oplysninger i AI-systemer
- Hvordan artikel 32 (sikkerhed) konkret skal operationaliseres
- Om der stilles krav om særlige kontrolforanstaltninger.

Behandling af helbredsoplysninger, sociale forhold eller strafbare forhold i AI-systemer indebærer betydelig retssikkerhedsmæssig risiko.

Vi finder derfor, at lovgivningen bør ledsages af klare krav om dokumenteret risikostyring og kontrol ved behandling af særlige kategorier af oplysninger.

5. Undtagelser fra registreredes rettigheder – manglende modgående kontrol

Lovforslaget åbner mulighed for undtagelser fra rettigheder i GDPR artikel 12 og 15–21 med hjemmel i artikel 23.

Der fastsættes imidlertid ikke:

- Krav om obligatorisk logning (jf. AI-forordningens artikel 12)
- Krav om dokumenteret kontrol med anvendelsen af undtagelser
- Krav om ekstern efterprøvelse.

Når borgerens mulighed for direkte kontrol reduceres, bør den strukturelle kontrol tilsvarende styrkes.

Vi finder derfor, at eventuelle undtagelser bør ledsages af krav om dokumenteret kontrol og mulighed for uafhængig assurance.

6. Symmetri med private aktører – manglende parallel kontrolstruktur

AI-forordningen (EU) 2024/1689 pålægger højrisiko-AI omfattende krav i artikel 9–15 om:

- Risikostyring
- Datastyring
- Teknisk dokumentation
- Logning
- Menneskeligt tilsyn
- Robusthed.

Private aktører vil være underlagt regulatorisk kontrol og markedsovervågning (kapitel VII).

Lovforslaget indeholder imidlertid ikke en tilsvarende eksplicit kontrolstruktur for offentlige myndigheder.

Vi finder det principielt problematisk, hvis offentlige myndigheder – som anvender AI i myndighedsudøvelse – ikke underlægges mindst tilsvarende krav til dokumentation og kontrol som private aktører.

7. Uafhængig tredjepartsassurance – et manglende, men oplagt supplement

Lovforslaget indeholder ikke bestemmelser om uafhængig tredjepartsverifikation.

Vi finder, at uafhængig assurance kan udgøre et proportionalt og effektivt supplement til eksisterende tilsyn.

FSR Danske Revisorer har tidligere udarbejdet vejledning for ISAE 3000-erklæringer vedrørende GDPR, som anvendes bredt i både offentlig og privat sektor.

Vi er aktuelt i færd med at udvikle en tilsvarende standard for AI-kontrol og AI-governance.

En erklæringsbaseret model vil kunne:

- Dokumentere overholdelse af AI-forordningens artikel 9–15
- Understøtte GDPR accountability
- Skabe ensartet kontrolformat
- Understøtte myndighedstilsyn.

Fraværet af en struktureret mulighed for tredjepartsassurance i lovforslaget fremstår som en væsentlig ubenyttet mulighed for at styrke retssikkerhed og tillid.

8. Bemærkning vedrørende tredjelandsoverførelser

Det fremgår udtrykkeligt af lovforslagets almindelige bemærkninger, at problemstillinger relateret til tredjelandsoverførelser efter databeskyttelsesforordningen ikke adresseres i forslaget.

Vi finder det relevant at fremhæve, at udvikling og anvendelse af AI-systemer i praksis ofte indebærer brug af cloudinfrastruktur, eksterne leverandører og tekniske miljøer, hvor behandling helt eller delvist kan finde sted uden for EU og EØS. Dette gælder navnlig i relation til træning, support og løbende systemforbedringer.

Selvom tredjelandsoverførelser er reguleret i databeskyttelsesforordningens kapitel V, indebærer lovforslaget etableringen af et supplerende nationalt retsgrundlag for behandling ved brug af AI. Når der samtidig åbnes for en bred anvendelse af AI i den offentlige forvaltning, bør de internationale databeskyttelsesretlige implikationer indgå som en tydelig del af den samlede retlige ramme.

Vi finder derfor, at det bør overvejes at præcisere i lovforslaget eller bemærkningerne, hvordan myndigheder forventes at håndtere tredjelandsoverførelser i AI-sammenhæng. En sådan præcisering vil ikke ændre ved GDPR's direkte anvendelighed, men vil styrke retssikkerheden og sikre en mere sammenhængende regulering.

9. Supplerende bemærkninger til det reviderede lovforslag

Det reviderede lovforslag udvider anvendelsesområdet til opgaver, der udføres i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, og præciserer bemyndigelsesbestemmelsen i § 3, stk. 2. Vi har to bemærkninger hertil:

Bemyndigelsesbestemmelsen i § 3, stk. 2

Bestemmelsen giver ressortministrene adgang til at fastsætte yderligere eller specifikke foranstaltninger, herunder tekniske og organisatoriske, men forpligter ikke til at tage stilling til, om sådanne foranstaltninger er påkrævede. Ved behandling af særlige kategorier af personoplysninger i AI-systemer er det efter vores opfattelse ikke tilstrækkeligt, at passende sikringsforanstaltninger kan fastsættes. Vi anbefaler, at der indføres et krav om, at den enkelte ressortminister skal vurdere og dokumentere, om der er behov for yderligere eller specifikke foranstaltninger inden for eget ressort, og at vurderingen gøres tilgængelig, så den kan efterprøves. Uden et sådant krav overlades ansvaret reelt til den enkelte dataansvarlige med den usikkerhed om fornødne garantier, som vi har påpeget i afsnit 4.

Definitionen af udvikling i § 2, nr. 5

Med udvidelsen af anvendelsesområdet får definitionen af udvikling i § 2, nr. 5, større rækkevidde. Definitionen fremstår uklar i forhold til de begreber, der anvendes i AI-forordningen, herunder sondringen mellem udbyder og idriftsætter samt mellem træning, videreudvikling og væsentlig ændring af et AI-system. Vi anbefaler, at definitionen afstemmes med AI-forordningens terminologi, så det er klart, hvornår en myndighed anses for at udvikle et system og dermed påtager sig udbyderforpligtelser.

De indsatte eksempler på lovforslagets anvendelsesområde og den mere detaljerede beskrivelse af behandling af særlige kategorier af oplysninger er en forbedring, men adresserer efter vores opfattelse fortsat ikke behovet for minimumsgarantier og dokumenteret kontrol, jf. afsnit 4. Til de øvrige ændringer af afgrænsning, viderebehandling og teknisk karakter har vi ingen bemærkninger.

10. Samlet vurdering

FSR Danske Revisorer støtter etableringen af et generelt retsgrundlag for offentlig anvendelse af AI.

Vi finder imidlertid, at lovforslaget i sin nuværende form:

- Udvider anvendelsesadgangen uden tilsvarende eksplicit kontrolramme
- Åbner mulighed for rettighedsbegrænsninger uden modgående strukturel kontrol
- Ikke sikrer symmetri med private aktørers dokumentationskrav.

Vi anbefaler derfor, at der i den videre lovbehandling indarbejdes eller præciseres krav om:

- Dokumenteret AI-governance
- Formaliseret risikostyring

- Krav om logning og sporbarhed
- Mulighed for uafhængig tredjepartsassurance.

Offentlig anvendelse af højrisiko-AI i myndighedsudøvelse forudsætter et robust, dokumenterbart og efterprøveligt kontrolgrundlag.

Vi står gerne til rådighed for dialog om udvikling af standardiserede kontrol- og erklæringsrammer for AI-anvendelse i både offentlig og privat sektor.

På vegne af FSR Danske Revisorers Cybersikkerhedsudvalg

Med venlig hilsen

FSR Danske Revisorer

GRO
QUMEA

København, 9. oktober 2026

Høringssvar fra GRO Capital A/S og QUMEA vedrørende udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Vi er opmærksomme på, at hverken GRO Capital A/S (GRO) eller QUMEA fremgår af høringslisten. På baggrund af vores forståelse for området, samt vores erfaring og indsigt som henholdsvis dansk investor og europæisk velfærdsteknologivirksomhed, ønsker vi alligevel at bidrage til et oplyst og balanceret lovforslag. Lovforslaget rummer efter vores opfattelse både betydelige muligheder, men også visse risici. Dette ser vi særligt, når digitale løsninger og AI anvendes i relation til monitorering af borgere – herunder patienter, pårørende og sundhedspersonale – i ofte intime og private situationer.

Lovforslagets formål og betydning for sundheds- og velfærdsområdet
Lovforslagets formål om at etablere klare og ensartede rammer for offentlige myndigheders udvikling og anvendelse af AI-systemer ved behandling af personoplysninger er efter vores opfattelse både relevant og rettidigt. Digitalisering og AI kan bidrage til at håndtere en række strukturelle udfordringer på sundheds- og velfærdsområderne, herunder den vedvarende mangel på arbejdskraft. Klare og forudsigelige lovgivningsmæssige rammer er efter vores opfattelse en forudsætning for, at det offentlige uden unødig administration kan træffe kvalificerede valg af nye teknologier og digitale løsninger, der både aktivt styrker borgernes velfærd, har en lav cybersikkerhedsrisiko og ikke unødigt kan opfattes som overvågning. Herved understøttes en mere effektiv og mindre risikofyldt implementering af digitale løsninger, som frigør ressourcer til kerneopgaven og bidrager til en bedre velfærd og sundhed.

Tryg og ansvarlig anvendelse på sundheds- og velfærdsområdet
Det er efter vores opfattelse afgørende, at anvendelsen af AI og digitale løsninger på sundheds- og velfærdsområdet tager udgangspunkt i borgernes oplevelse af tryghed, værdighed og tillid. Teknologiske løsninger bør styrke den faglige kvalitet og må ikke forværre borgernes helbredstilstand eller oplevelse af den offentlige service eller teknologien. Dette ikke alene af hensyn til patienter og de ældre borgere, men også pårørende og medarbejdere, som skal kunne have tillid til, at de teknologier der anvendes, understøtter en værdig og ansvarlig behandling og pleje, et meningsfuldt hensyn til pårørende, og et trygt arbejdsmiljø, og ikke fungerer som fx patient- eller medarbejderovervågning.

Vores forståelse er, at lovforslaget har et fokus på, hvilke personoplysninger der behandles, og at behandlingen skal være nødvendig og proportional ift. GDPR's principper om bl.a. dataminimering, integritet og fortrolighed. Efter vores opfattelse bør databeskyttelse imidlertid ikke alene indgå i vurderingen af, hvordan personoplysninger behandles, men også ved udformningen og valget af den teknologi, der anvendes. Lovforslaget bør tydeliggøre ønsket om øget anvendelse af kunstig intelligens og digitale løsninger med hensynet til privatliv og datasikkerhed. Overvejelserne om datasikkerhed og databeskyttelse bør således indgå som en integreret del af vurderingen af teknologiernes anvendelse og proportionalitet. En styrende tilgang bør fx være, at et givent klinisk eller plejefagligt formål tilstræbes opnået med både påvist nytteværdi og den mindst mulige behandling af persondata og dermed den mindst mulige indgriben i borgerens, pårørendes og medarbejdernes liv

GRO og QUMEA anbefaler derfor, at der i loven til § 3 præciseres, at myndigheder ved vurderingen af nødvendighed og proportionalitet også bør forholde sig til, om det tilsigtede formål kan opnås med en mindre indgribende teknologisk løsning og med mindre behandling af personoplysninger.

Monitorering og risikoprofil
Efter vores vurdering kan anvendelse af AI på sundheds- og velfærdsområdet have konsekvenser for borgernes privatliv og oplevelse af værdighed, hvis det anvendes uden tilstrækkelig hensyntagen til kontekst og borgergruppe – stik imod det, som vi også forstår, er den ønskede udvikling af sundhed- og velfærdsområdet.

Herunder er det vigtigt at være opmærksom på, at teknologier på fx monitoreringsområdet varierer i deres risikoprofil. Løsninger baseret på billed- eller lydoptagelser indebærer generelt en højere grad af indgriben for borgere og personalet, både fordi de kan opleves som overvågning, og fordi eventuelle datasvigt kan afsløre meget følsomme oplysninger om borgernes adfærd i intime situationer, på trods af eventuel efterbehandling af data med henblik på fjernelse af personfølsom information. Omvendt kan data, der aldrig indsamles i en form, der gør det muligt at identificere den enkelte, ikke blive udsat for risiko, selv ikke i tilfælde af uautoriseret adgang.

Den teknologiske udvikling på området har medført, at der i dag findes løsninger, som udelukkende registrerer bevægelses- eller tilstedeværelsesmønstre uden brug af optisk registrering (video) eller lydoptagelser, uden at der på noget tidspunkt er mulighed for identifikation af den enkelte borger og uden at der produceres data, der kan tilbageføres til borgeren. Sådanne løsninger kan i mange tilfælde understøtte samme formål med en markant lavere grad af indgriben i privatlivet og med reducerede risici i forhold til datasikkerhed. Da der hverken genereres billeder eller lyd, kan sådanne systemer heller ikke bruges til at overvåge personalet. Denne skelnen anerkendes i stigende grad andre steder i Europa. Etiske organer, regeringer og databeskyttelsesmyndigheder i andre lande har i nylige vejledninger anvendt det samme princip, fx Schweiz.

Opsummerende bør det være et centralt hensyn i lovbemærkningerne, at nye teknologier indføres på en måde der bevarer borgernes følelse af integritet og opleves som tryghedsskabende frem for overvågende. Dette er særligt relevant blandt udsatte borgere med fx demens eller andre diagnoser, hvor der er en påvist negativ effekt af oplevelsen af overvågning, der direkte kan modvirke formålet med et behandlingsforløb.

Vi finder det derfor positivt, at lovforslagets bemærkninger fremhæver, at anvendelse af AI over for særligt sårbare grupper taler for at overveje, hvordan det højest mulige beskyttelsesniveau kan sikres.

Regulering, MDR og behovet for nærmere afklaring

Når AI og teknologier anvendes på sundheds- og velfærdsområdet til fx at opdage ændringer i borgernes helbredstilstand, monitorere kliniske parametre eller på anden måde understøtte plejepersonalets faglige vurderinger, er det væsentligt at sikre, at EU-reglerne om medicinsk udstyr (MDR) efterleves, og at udstyret er CE-mærket og godkendt som medicinsk udstyr efter gældende regler. På denne måde kan borgere, pårørende og medarbejdere have tillid til, at de teknologier der anvendes, lever op til de samme krav til sikkerhed, dokumentation og pålidelighed som andet medicinsk udstyr. Dette er ikke mindst relevant i den nuværende cybersikkerhedsituation hvor adskillige analyser og rapporter peger på øget risiko ved fx kinesiske komponenter. Kommuner og institutioner bør derfor have fuld transparens i, hvilke komponenter de indkøber til brug i deres velfærdsinstitutioner.

Efter vores opfattelse vil det være en styrkelse af lovforslaget, hvis samspillet mellem lovforslaget og bl.a. MDR tydeliggøres i lovbemærkningerne og tænkes ind i det efterfølgende arbejde. Lovforslaget lægger op til, at ressortministrene kan fastsætte passende og specifikke beskyttelsesforanstaltninger på deres respektive områder. Vi ser, at særligt på sundheds- og ældreområdet, hvor anvendelsen af AI kan indebære behandling af særlige kategorier af personoplysninger, herunder helbredsoplysninger, er der behov for klare sektorspecifikke rammer. En sådan præcisering i lovbemærkningerne vil kunne understøtte det offentliges indkøb og implementering af nye teknologier og samtidig reducere risikoen for valg af løsninger, der kan indebære juridisk, klinisk eller operationel usikkerhed.

GRO og QUMEA opfordrer derfor til, at Forsknings-, Uddannelses- og Digitaliseringsministeriet i det videre arbejde er i dialog med de relevante ressortministerier med henblik på at tydeliggøre grænsefladerne mellem AI-hjemmelsloven, sektorspecifik regulering og for at afklare grænseflader mellem teknologityper og derved sikre fagligt bæredygtige løsninger. Desuden, at Forsknings-, Uddannelses- og Digitaliseringsministeriet i sin dialog med de relevante ressortministerier bidrager til at sikre, at EU-reglerne om medicinsk udstyr (MDR) overholdes. GRO og QUEMA anbefaler, at den generelle AI-hjemmel følges op af en sektorspecifik bekendtgørelse for sundheds- og ældreområder, som fastlægger klarere rammer for myndighedernes anvendelse og indkøb, når der er tale om AI-løsninger, som kræver

CE-mærkning og MDR godkendelse.

Afslutningsvis skal det bemærkes, at GRO og QUMEAs ønske med nærværende høringssvar er at bidrage til et oplyst og balanceret lovforslag.

Vi håber, at vores bemærkninger kan indgå konstruktivt i det videre arbejde og står naturligvis til rådighed for yderligere dialog, hvis det måtte være relevant.

Med venlig hilsen

Lars Lunde, GRO Capital A/S.
Hans Erik Henriksen, QUMEA Danmark.

07.10.26

Vedr. fornyet høring over udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

HK takker for muligheden for at afgive bemærkninger til det reviderede forslag til AI-hjemmelslov.HK støtter, at der skabes et klarere og mere ensartet retsgrundlag for offentlige myndigheders og organers brug af AI. Uklarhed om hjemlen må ikke i sig selv stå i vejen for en ansvarlig anvendelse af ny teknologi, der kan styrke kvaliteten i den offentlige sektor.

Det reviderede lovforslag indeholder også relevante forbedringer. Det er blandt andet blevet tydeligere, at AI kan bruges som beslutningsstøtte, men at den menneskelige involvering skal være reel. En medarbejder, der alene overtager AI-systemets forslag uden selvstændigt at tage stilling til det, opfylder efter bemærkningerne ikke kravet om reel menneskelig beslutningsstøtte.

HK mener samtidig, at en bredere og klarere hjemmel stiller større krav til den konkrete implementering ude i myndighederne. Loven løser i høj grad spørgsmålet om, hvornår der er hjemmel til at bruge AI på personoplysninger. Den løser ikke i samme grad spørgsmålet om, hvordan AI skal indarbejdes i arbejdsgange, ledelse, kontrol, dokumentation og medarbejdernes opgaver.

Det er afgørende. Ellers risikerer man at løse hjemmelsproblemet uden at løse implementeringsproblemet.

HK DANMARK
TELEFON +45 7011 4545
hk@hk.dk

Weidekampsgade 8
DK-2300 København S

HK.DK

1. En bred hjemmel kræver klare rammer og tydeligt ledelsesansvar

Lovforslaget tager nu udgangspunkt i, at offentlige myndigheder og organer kan anvende loven, når behandlingen af personoplysninger sker efter databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Det skaber større klarhed. Men det betyder samtidig, at meget af den konkrete vurdering af, hvordan AI skal bruges forsvarligt, ligger hos den enkelte myndighed.

HK mener derfor, at det skal være tydeligt, at ansvarlig brug af AI ikke alene er et spørgsmål for den enkelte medarbejder. Det er først og fremmest et ledelses- og organisationsansvar.

Før et AI-system bruges i sagsbehandlingen, bør myndigheden som minimum have taget stilling til:

- hvilke opgaver systemet må bruges til
- hvilke opgaver det ikke må bruges til
- hvem der har det ledelsesmæssige ansvar
- hvilke risici der er for borgere og medarbejdere
- hvilke datagrundlag AI-systemet bygger på
- hvilke oplysninger systemet må behandle
- hvilke kontrolpunkter der skal være
- hvad der skal dokumenteres
- hvilke kompetencer medarbejderne skal have
- hvordan fejl, tvivl og afvigelser skal håndteres.

HK foreslår derfor, at loven følges af fælles nationale minimumskrav til myndighedernes governance og implementering af AI.

Det bør ikke være op til den enkelte medarbejder at kompensere for manglende organisatoriske rammer.

2. Reel menneskelig kontrol skal sikres i arbejdsgangen

HK ser positivt på, at det nye lovforslag tydeligere beskriver, at et menneske reelt skal forholde sig til AI-systemets anbefalinger.

Bemærkningerne peger også på, at reel menneskelig involvering kan understøttes ved at fastlægge beslutningskompetencen, dokumentere

afvigelser fra AI-systemets anbefalinger og sikre relevant logning. Det fremgår imidlertid samtidig, at disse procedurer ikke i sig selv er krav efter loven.

Det efterlader efter HK's opfattelse et vigtigt hul.

Der er forskel på, om en medarbejder formelt har mulighed for at ændre et AI-forslag, og om arbejdsgangen reelt er indrettet sådan, at medarbejderen forventes og gives mulighed for at kontrollere det.

Hvis systemet præsenterer et færdigt forslag, tidspresset er stort, kontrollen ikke dokumenteres, og medarbejderen ikke har adgang til det nødvendige grundlag, kan der opstå en risiko for, at AI-systemets forslag bliver godkendt mere eller mindre automatisk.

HK foreslår derfor, at der stilles krav om dokumenterede menneskelige kontrolpunkter, når AI-output får betydning for en afgørelse eller et væsentligt tiltag over for en borger.

Arbejdsgangen bør være indrettet, så medarbejderen faktisk skal tage stilling og ikke alene trykke godkend.

3. Kompetencer er et organisationsansvar

Reel menneskelig kontrol kræver kompetencer.

Men kompetencer handler ikke kun om at have gennemført et generelt kursus i AI. Medarbejderen skal kunne forstå, hvad systemet bruges til, hvilke begrænsninger det har, hvilke fejl der kan opstå, og hvad der skal kontrolleres i den konkrete faglige sammenhæng.

AI-forordningens artikel 4 kræver, at udbydere og idriftsættere af AI-systemer træffer foranstaltninger til at understøtte medarbejdernes AI-færdigheder. Bestemmelsen kræver imidlertid ikke, at organisationen garanterer et bestemt niveau af AI-færdigheder hos den enkelte medarbejder.

Det gør det efter HK's opfattelse endnu vigtigere, at de konkrete kompetencekrav bliver taget alvorligt i forbindelse med offentlig sagsbehandling.

Medarbejderen skal ikke alene have viden. Medarbejderen skal også have tid, information, støtte og reel mulighed for at tilsidesætte AI-systemets anbefaling.

HK foreslår, at myndigheder før ibrugtagning af AI-systemer skal fastlægge, hvilke konkrete kompetencer der kræves for de medarbejdere, der skal anvende og kontrollere systemet, og hvordan disse kompetencer sikres og vedligeholdes.

Det skal samtidig stå klart, at medarbejdere ikke må stå med ansvaret for fejl, der i virkeligheden skyldes mangelfuld implementering, manglende oplæring eller utilstrækkelige arbejdsgange.

4. Der skal kunne følges et beslutningsspor

Når AI får betydning for sagsbehandlingen, skal det efterfølgende være muligt at forstå, hvad der er sket.

Lovforslaget nævner relevant logning som en måde at understøtte og dokumentere reel menneskelig involvering på, men gør ikke logning til et generelt krav.

HK mener, at sporbarhed er en nødvendig del af ansvarlig AI-anvendelse.

Det skal ikke nødvendigvis betyde, at enhver teknisk handling skal gemmes for altid. Men hvis AI har haft betydning for en sag, bør det efterfølgende kunne dokumenteres, hvilket system der blev brugt, hvilket relevant output det gav, og hvordan medarbejderen forholdt sig til det.

Det har betydning for borgerens mulighed for at forstå og anfægte en afgørelse. Det har også betydning for medarbejderens mulighed for at dokumentere sin egen faglige vurdering.

HK foreslår derfor, at der fastsættes krav om relevant logning og sporbarhed, når AI indgår i sagsbehandlingen på en måde, der har betydning for en borgers sag.

5. Der er brug for klare regler om notat- og journaliseringspligt

Lovforslaget lægger til grund, at forvaltningsloven og offentlighedsloven er teknologineutrale og fortsat gælder, når AI anvendes.

Det er juridisk vigtigt, men det giver ikke i sig selv tilstrækkeligt klare svar på, hvordan reglerne skal bruges i nye AI-understøttede arbejdsgange.

Det bliver særligt tydeligt, når AI ikke alene producerer et tekstudkast, men foretager handlinger i et sags- eller journalsystem.

Hvis en AI-agent for eksempel søger i et journalsystem, finder flere hundrede dokumenter og sorterer en del af dem fra som interne i forbindelse med en aktindsigtssag, opstår en række konkrete spørgsmål:

Hvordan dokumenteres søgningen og frasorteringen? Hvad skal medarbejderen kontrollere? Hvad skal gemmes? Og hvordan kan man efterfølgende se, hvilke dokumenter der blev vurderet?

Ombudsmandens praksis om journalisering understreger allerede betydningen af dokumentation af, hvilke dokumenter og oplysninger der er vurderet i forbindelse med aktindsigt.

Det er derfor ikke tilstrækkeligt blot at konstatere, at de eksisterende regler er teknologineutrale.

HK foreslår, at der udarbejdes en fælles national vejledning om notat- og journaliseringspligt ved brug af generativ og agentbaseret AI.

Vejledningen bør blandt andet tage stilling til AI-genererede udkast, opsummeringer, klassifikationer, søgninger, frasorteringer, anbefalinger og relevante logs.

6. Ombudsmandens aktuelle undersøgelse understreger behovet for klare rammer

Folketingets Ombudsmand har i august 2026 iværksat en række høringer af udvalgte kommuner om deres brug af AI i blandt andet borgerkontakt og sagsbehandling.

Ombudsmanden spørger blandt andet til kommunernes brug af AI i direkte kontakt med borgere og til AI-værktøjer, der understøtter sagsbehandlingen. Kommunerne bliver også bedt om at redegøre for, hvordan de sikrer, at blandt andet vejledningspligt, notatpligt og saglighed bliver

overholdt. Ombudsmanden har samtidig oplyst, at myndighedernes brug af AI vil være et fokusområde i de kommende år.

HK mener ikke, at den igangværende undersøgelse kan bruges som dokumentation for, at kommunerne generelt anvender AI forkert. Undersøgelsen viser derimod, at der er aktuelle og konkrete spørgsmål om, hvordan de almindelige forvaltningsretlige krav skal sikres i praksis, når AI bliver en del af sagsbehandlingen.

Det taler efter HK's opfattelse for, at en generel AI-hjemmel bør følges af fælles og operationelle rammer for anvendelsen.

7. Viderebehandling af eksisterende borgersager kræver klare garantier

Lovforslaget åbner for, at myndigheder kan bruge personoplysninger, som de allerede lovligt behandler, til udvikling af AI-systemer. Det omfatter også oplysninger fra historiske og afsluttede sager.

Lovforslaget skal i den forbindelse gøre det unødvendigt at foretage en konkret forenelighedstest efter databeskyttelsesforordningens artikel 6, stk. 4, før oplysninger fra historiske og lukkede sager viderebehandles til udvikling af AI-systemer.

Det betyder ikke, at databeskyttelsesreglerne i øvrigt sættes ud af kraft.

Men det betyder, at en konkret kontrol af formålsskiftet erstattes af den generelle hjemmel i loven. Derfor bliver det endnu vigtigere, at der er andre klare garantier.

HK foreslår, at myndigheden, før eksisterende borgersager bruges til udvikling eller træning af AI, skal dokumentere:

- hvorfor oplysningerne er nødvendige
- hvilke oplysninger der skal anvendes
- om datamængden kan begrænses
- om oplysninger kan anonymiseres eller pseudonymiseres
- hvilke risici anvendelsen indebærer
- hvordan risikoen for bias og forskelsbehandling håndteres
- proces for løbende opdatering af data
- løbende overvågning af om AI-systemet ændrer adfærd over tid

Der bør være særlig opmærksomhed på følsomme oplysninger og oplysninger om borgere i udsatte eller sårbare situationer.

8. Begrænsning af borgernes rettigheder

HK noterer sig positivt, at § 4 i det reviderede lovforslag nu tydeligere fastslår, at rettigheder efter databeskyttelsesforordningens artikel 12 og artikel 15-21 kan begrænses helt eller delvist, og kun hvis betingelserne i artikel 23 er opfyldt.

HK mener samtidig, at centrale garantier for borgerne så vidt muligt bør fremgå direkte af loven og ikke alene overlades til efterfølgende bekendtgørelser.

Jo større betydning AI får i offentlig sagsbehandling, desto vigtigere bliver muligheden for at forstå og efterprøve myndighedens beslutninger.

HK foreslår derfor, at det præciseres, at en begrænsning skal kunne begrundes konkret og dokumenteres som nødvendig og proportional, og at borgerens muligheder for klage og efterprøvelse skal sikres.

9. Bias og historiske data

Ministeriet peger selv på risikoen for, at AI-systemer kan indeholde bias. Det fremgår også af lovbemærkningerne, at historiske datasæt kan indeholde skævheder, som AI kan videreføre eller forstærke, herunder over for sårbare grupper.

Denne risiko bliver særlig relevant, når lovforslaget samtidig åbner for anvendelse af historiske sager til udvikling af AI.

Det kan i praksis være vanskeligt for både en borger og en medarbejder at opdage, at en systematisk skævhed har påvirket en anbefaling.

HK noterer sig, at hjemlen alene omfatter oplysninger, som myndigheden fortsat lovligt opbevarer, og ikke giver adgang til at forlænge opbevaringstiden alene med henblik på fremtidig AI-udvikling

HK foreslår derfor, at relevante AI-systemer skal testes for skævheder før ibrugtagning og følges løbende efter ibrugtagning.

Myndigheden bør have en klar procedure for at undersøge fejl og klager og for at ændre eller stoppe en AI-anvendelse, hvis der konstateres systematiske problemer.

10. Effektivisering kræver investering

HK anerkender, at AI kan frigøre tid og styrke kvaliteten i den offentlige sektor.

Men AI skaber også nye opgaver.

Der skal blandt andet bruges ressourcer på dataklargøring, test, kvalitetssikring, support, dokumentation, opkvalificering, menneskelig kontrol og løbende vedligeholdelse.

HK finder derfor, at lovbemærkningernes forventninger om betydelige effektiviseringsgevinster bør nuanceres.

HK foreslår, at effektiviseringsgevinster først lægges til grund, når løsningerne er afprøvet i praksis, og når både gevinster og nye følgeopgaver er dokumenteret.

Medarbejderne bør inddrages tæt i udvikling og afprøvning, før gevinster indregnes. Det er medarbejderne, der kender arbejdsgangene og kan se, hvor AI faktisk sparer tid, og hvor teknologien skaber nye opgaver.

11. Fælles rammer skal følge med den fælles hjemmel

Et vigtigt formål med lovforslaget er at skabe mere ensartede regler for myndighedernes brug af AI.

HK mener, at denne ensartethed ikke bør stoppe ved selve hjemlen.

Hvis alle myndigheder får samme brede hjemmel, men hver kommune, region og statslig myndighed bagefter selv skal afgøre, hvordan menneskelig kontrol, logning, journalisering, kompetencer og AI-agenter skal håndteres, risikerer man blot at flytte usikkerheden fra hjemmelsspørgsmålet til implementeringen.

HK foreslår derfor, at der inden eller i tæt forbindelse med lovens ikrafttræden udarbejdes et samlet nationalt vejledningsmateriale med fælles minimumsstandarder.

Det bør som minimum omfatte:

- ledelsesansvar og godkendelse af AI-anvendelser
- reel menneskelig kontrol
- medarbejdernes kompetencer
- dokumentation og sporbarhed
- logning
- notat- og journaliseringspligt
- generativ og agentbaseret AI
- brug af eksisterende personoplysninger til udvikling og træning.

12. Loven bør evalueres

AI udvikler sig hurtigt, og lovforslaget giver mulighed for en bred anvendelse på tværs af den offentlige sektor.

HK foreslår derfor, at loven evalueres efter to år.

Evalueringen bør ikke alene se på, hvor meget AI der bliver anvendt, eller om der er opnået økonomiske gevinster.

Den bør også undersøge:

- fejl og klager
- borgernes retssikkerhed
- om menneskelig kontrol fungerer reelt
- hvor ofte medarbejdere afviger fra AI-anbefalinger
- bias og diskrimination
- brugen af historiske borgersager
- dokumentations- og journaliseringspraksis
- medarbejdernes kompetencer og arbejdsvilkår
- ressourceforbruget ved kontrol og kvalitetssikring
- anvendelsen af mulighederne for at begrænse registreredes rettigheder.

Afsluttende bemærkninger

HK støtter ønsket om klare rammer for brug af AI i den offentlige sektor.

En generel hjemmel kan fjerne en væsentlig juridisk usikkerhed og give mulighed for at bruge AI dér, hvor teknologien kan styrke kvaliteten og understøtte medarbejdernes arbejde.

Men hjemlen kan ikke stå alene.

Jo bredere muligheder myndighederne får for at anvende AI, desto vigtigere er det, at ledelse, arbejdsgange, kompetencer, dokumentation og kontrol er på plads.

Reel menneskelig kontrol må ikke blive et krav, som i praksis alene placeres hos den enkelte medarbejder. Det skal være indbygget i den måde, organisationen vælger, indfører og anvender AI-systemer på.

Ellers er der risiko for, at mangler i organisationens implementering først bliver synlige, når en medarbejder begår en fejl, eller en borger bliver ramt af en forkert eller uigennemsigtig beslutning.

HK opfordrer derfor til, at den generelle hjemmel ledsages af fælles, konkrete og anvendelige rammer for ansvarlig brug af AI i den offentlige sektor.

Teknologi-
vurdering

Til Digitaliseringsstyrelsen
Landgreven 4
1017 København K
att. jonmei@digst.dk
emimoi@digst.dk
leaomd@digst.dk
kahevi@digst.dk

11. oktober 2026

Høringssvar til udkast til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

IDA Teknologivurdering takker for muligheden for at afgive høringssvar. Lovforslaget adresserer et presserende behov for rammer omkring brugen (AI) i offentlige myndigheder og organer, men i sin nuværende ganske åbne og uklare form rejser forslaget væsentlige bekymringer.

IDA Teknologivurdering er et fagligt selskab tilknyttet Ingeniørforeningen i Danmark og har medlemmer, der arbejder som ingeniører i offentlig forvaltning, private virksomheder og forskningsinstitutioner. Selskabet beskæftiger sig især med relationen mellem teknologier og deres samfundsmæssige anvendelse, herunder påvirkning af teknologisk udvikling og teknologiers betydning for sociale, økonomiske og politiske forhold.

IDA Teknologivurderings overordnede vurdering er, at lovforslaget lægger op til en alt for bred og generel hjemmel, uden at de nødvendige retsgarantier for borgerne er sikret i lovteksten. Lovens fokus er helt overvejende at sikre, at de eksisterende bestemmelser i EU-retten og i dansk lovgivning om følsomme personoplysninger overholdes, men tager ikke højde for, at den udvikling og anvendelse af AI, som loven hjemler i høj grad må forventes at påvirke de offentlige myndigheders og organers sagsbehandling samt de kriterier, der lægges til grund for afgørelser i denne sammenhæng. Desuden hjemler loven mulighed for at der kan gennemføres screeninger og profilering af borgere hvis sigte er at imødegå ikke retmæssig brug af ydelser fra det offentlige. I stedet overlades kritiske beskyttelsesmekanismer til fremtidige ministerielle bekendtgørelser.

AI i sagsbehandling adskiller sig grundlæggende fra traditionelle IT-værktøjer, der arbejder med udgangspunkt i offentlige registre og fagligt anerkendt praksis og evidens. Det særlige ved AI-systemerne er deres udvidede datagrundlag og udstrakte brug af beregnede sandsynligheder, som både kan sløre beslutningsgrundlaget og har vist sig at reproducere historiske skævheder.

Skal tilliden til myndighedsudøvelsen bevares, er det afgørende, at kravene både til involvering af kompetent, menneskelig sagsbehandling, gennemsigtighed i grundlaget for valg

og afgørelser og en udvidet leverandørstyring skrives direkte ind i selve loven og gøres gælder for hele systemernes livscyklus fra forsøg, over udvikling til anvendelse.

Nedenfor følger IDA Teknologivurderings syv hovedpunkter og anbefalinger til lovforslaget:

De særlige egenskaber ved AI

Et AI-system forstår ikke en sag, de forhold af personlig, sundhedsmæssige eller anden karakter, der indgår i den og de mennesker, den handler om. Det beregner det sandsynlige svar ud fra mønstre i data, og et velformuleret svar er derfor ikke det samme som et korrekt svar. Systemerne afspejler de data, der har været inddraget i processen, og de menneskelige vurderinger, de er trænet på. Trænes de på en myndigheds gamle sager, kan tidligere skævheder og fejl blive ført videre, som det også noteres i bemærkningerne til loven.

AI-systemer, som de rimeligt er defineret i lovens §2 stk. 1 med påpegning af autonomi, tilpasningsevne samt at foretage afvejninger gennem fx ved benyttelse af algoritmer, der kan optræde som beslutnings- og handlingsagenter, kan trænes, men også kan optræde med læring på basis af data, og dermed kan skabe forudsigelser, opstille anbefalinger og foreslå beslutninger. Disse forhold gør, at AI-systemer ikke lever op til at være teknologineutrale i den økonomiske og juridiske forståelse, som loven opererer med.

AI-systemers transparens og sporbarheden af forudsigelser, anbefalinger og beslutninger begrænses af både anvendelsen af statistisk mønstergenkendelse og af sprogalgoritmer. Dette forhold skærpes yderligere af, at der ikke loven er angivet præcise krav til, at det datagrundlag, der benyttes af et AI-system, skal være præciseret. Mens brugen af lærende algoritmer på veldefinerede registre, tidligere afgørelser og datakilder, som fx videnskabelig litteratur, kan sløres af de algoritmer til mønstergenkendelse, de anvendes, bliver inddragelse af data internettet og sociale medier en yderligere udfordring for det krav om transparens, der må stilles til offentlige myndigheders og organers beslutninger.

Det udelukker ikke anvendelse af AI, men loven bør tydeligt fastslå, at myndigheder skal være i stand til at redegøre både for de AI-procedurer, der anvendes, og det datamateriale, der indgår. Bemærkningerne til loven bør tydeligere beskrive systemernes begrænsninger, ikke kun deres muligheder.

Generel hjemmel, men frivillige garantier

Jo bredere en hjemmel er, desto stærkere bør garantierne stå i selve loven, hvilket de ikke gør. Loven giver alle offentlige myndigheder, organer og domstole en bred hjemmel til at udvikle og bruge AI, herunder til beslutningsstøtte og profilering af borgere. De garantier, der skal beskytte borgeren, er derimod i vid udstrækning overladt til de enkelte resortministre, som har mulighed for ud fra myndighedens egen vurdering og erfaring at fastsætte disse garantier, samt overlade det til at være et resultat af den praksis, der udvikles. I yderste tilfælde overlades det til afklaring gennem retsafgørelser.

Samtidig forudsætter forslaget, at gældende ret er tilstrækkelig. Bemærkningerne erkender dog selv, at lovgivningen ikke giver garantier mod forskelsbehandling, at kravet til menneskelig involvering ikke er afklaret, og at AI i sagsbehandling er grundlæggende forskellig fra traditionel sagsbehandling. Det gør sammenligningen med almindeligt kendte elektroniske hjælpemidler misvisende.

Kyndig sagsbehandling og menneskelig medvirken skal være reel og stå i loven

I dag er det kun bemærkningerne, ikke lovteksten, der klart udelukker rent automatiske afgørelser. Myndighederne gives således i §3, stk. 1 adgang til at benytte AI til beslutningsstørre, der i § 1 stk. 4 er defineret ved, at indebære, at AI-systemet ikke selv træffer afgørelsen eller iværksætter tiltaget. Det indebærer, at kravet om, at et kompetent menneske kan "inddrage" AI's forslag, kan opfyldes rent formelt. Reel medvirken kræver mere: en medarbejder, der er uddannet inden for det konkrete sagområde, som afgørelsen henter viden om, og det konkrete systems funktion, begrænsninger og fejlrisici, samt ikke mindst har tid og praktisk mulighed for at vurdere sagen, og som reelt har mandat til at afvige fra forslaget.

Risikoen for, at travle medarbejdere vælger at stole på AI-systemets forslag (automation bias), er anerkendt af Datatilsynet. Det understøttes af den forventning, der også udtrykkes i bemærkningerne til loven om betydelige personalebesparelser, som følge af udvikling og anvendelse af AI. Derfor bør logning og dokumentation af afvigelser være et lovkrav, så tilsynsmyndigheder kan kontrollere, om den menneskelige kontrol er reel. Grænsen til rent automatiske afgørelser er uafklaret og bør præciseres under hensyn til EU-Domstolens praksis. Kravet om menneskelig vurdering bør desuden gælde alle anvendelser, der i praksis kan påvirke en afgørelse – herunder også sagsforberedelsen.

Hele livscyklussen er afgørende: metode, data og resultater

Et AI-systems virkning afhænger af tre ting: de benyttede AI-metoder, karaktering af det benyttede datagrundlaget og i hvilket regi, systemerne udvikles og benyttes. Lovforslaget er stort set tavst om både kravene til og transparensen af det benyttede datagrundlag og om den kontekst, som systemudviklingen og -afviklingen sket i, hvilket bl.a. indebærer hvilke 'tredjeparter', der han adgang til data og resultater. Screeninger, profileringer og prioriteringer er oplysninger, systemet selv skaber, og de kan i sig selv afsløre både personfølsomme og sagsmæssige forhold. Det er uklart, hvordan sådanne afledte oplysninger er omfattet, hvor længe de må opbevares, om de må anvendes til andre formål og hvem, der må have adgang til processer og resultater.

Lovforslaget bør ud over at præcisere, hvem der må have adgang til systemer, data og resultater, desuden omfatte gentræning efter ibrugtagning. Indgår resultaterne som nye træningsdata, kan fejl og skævheder forstærke sig selv. Myndigheden bør derfor altid kunne dokumentere metode, datagrundlag og håndtering af resultater.

Borgerens retssikkerhed, transparens, leverandørforhold og bias

Borgeren skal have besked, når AI har indgået i en sag, og afgørelsens begrundelse skal specifikt redegøre for den rolle som AI har spillet. At et system har anbefalet en bestemt afgørelse, udgør ikke en juridisk begrundelse i sig selv. Retten til at få adgang til grundlaget for en myndigheds sagshåndtering eller afgørelse bør ikke kunne begrænses for den enkelte borger.

Lovforslaget lægger dog op til, at ministre får adgang til at begrænse borgerens rettigheder – blandt andet fordi det kan være teknisk umuligt eller gå ud over systemets præcision at opfylde dem. Systemets præcision er imidlertid primært et driftsøkonomisk eller teknisk hensyn. Begrænsninger af borgerens rettigheder bør derfor kun kunne indføres på helt konkrete områder og på baggrund af en forudgående konsekvensvurdering. Alle bekendtgørelser, der fastsætter garantier eller begrænsninger, bør sendes i offentlig høring, og ikke kun til Datatilsynet.

Myndigheder bør desuden forpligtes til at vurdere leverandørens jurisdiktion og have en klar exit-strategi, så de ikke fanges i kritisk leverandørafhængighed (vendor lock-in). Lovforslaget adresserer heller ikke dette spørgsmål.

Bias er en indbygget risiko, især når systemer trænes på historiske sager og/eller involverer data fra åbne og udokumenterede datakilder. Lovforslaget overlader det til den enkelte myndighed selv at håndtere denne risiko. Der bør i stedet stilles generelle krav om, at der ved udvikling af nye AI-systemer stilles gennemføres test for skævvridning før ibrugtagning samt løbende stikprøvekontrol i drift.

Konsekvensvurdering, ikrafttræden og evaluering

Lovforslagets konsekvensvurdering anser forebyggelse af snyd og fejl for at være uden relevans, selvom netop fejlrisikoen er en af de helt centrale udfordringer ved AI. Den vurdering bør revideres.

Lovforslaget lægger op til, at loven træder i kraft dagen efter bekendtgørelsen, hvilket sker på et tidspunkt, hvor EU's krav til højrisikosystemer (AI Act) endnu ikke er fuldt trådt i kraft. Der bør derfor indføres en overgangsordning eller et krav om, at tilsvarende garantier skal være på plads, før systemerne må tages i brug. Endelig bør loven evalueres efter tre år med tæt inddragelse af tilsynsmyndigheder og et klart borgerperspektiv.

Økonomiske og miljømæssige konsekvenser

I bemærkningerne til loven angives det, at der ikke er viden om de økonomiske og miljømæssige konsekvenser af øget inddragelse af AI hos offentlige myndigheder og organer. Der er fortsat usikkerheder på dette område, men der er næppe tvivl om, at netop udbredelsen af AI vil have alvorlige konsekvenser for el- og materialeforbrug – endog i et omfang, som viser sig væsentligt større end forventet. Dette punkt bør derfor løbende følges op og blive belyst, da en del tyder på, at de besparelser i offentlig forvaltning, som synes af være drivende for den øgede anvendelse af AI-systemer, modsvares af nye typer meget tidskrævende opgaver ved offentlige myndighedsafgørelser og store miljø- og klimaeffekter, der meget vel kan gøre gevinsterne ubetydelige.

Samlede anbefalinger

Den brede hjemmel skal ledsages af bindende minimumsgarantier i selve lovteksten, ikke kun af ministerielle bemyndigelser. Rent automatiske afgørelser skal udelukkes i loven, og beslutningsstøtte skal kræve en reel og selvstændig menneskelig vurdering, der understøttes af de rette kompetencer, tid, mandat og logning. Kravet bør gælde alle anvendelser, der kan påvirke en afgørelse, og reguleringen skal omfatte hele livscyklussen – herunder særligt resultater og gentræning.

Med venlig hilsen,

Michael Søgaard Jørgensen
2125 6815, msjo@plan.aau.dk
forperson, IDA Teknologivurdering

Ulrik Jørgensen
2166 5424, ulrik@sts-research.dk

Niels Johan Juhl-Nielsen
3095 6815, nielsjohan@gmail.com

bestyrelsesmedlemer, IDA Teknologivurdering

Ingeniørforeningen, IDA
Kalvebod Brygge 31-33
DK-1780 København V
Tlf. +45 33 18 48 48

ida.dk

Digitaliseringsstyrelsen
Att: jonmei@digst.dk,
kahevi@digst.dk
emimol@digst.dk
og leaomd@digst.dk

Svar på høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

9. oktober 2026

Hermed IDA's svar på høring vedr. forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Opsummering

IDA takker for muligheden for at afgive høringssvar.
IDA finder det meget positivt, at der skabes et tydeligere retsgrundlag for offentlige myndigheders og organers mulighed for at udvikle og anvende AI-systemer.
IDA er overordnet positiv overfor, at offentlige myndigheder inden for rammerne af deres fastlagte og afgrænsede opgaver kan anvende AI, også når det involverer behandling personoplysninger, herunder til beslutningsstøtte.
IDA finder det vigtigt, at de gældende regelsæt, ikke mindst databeskyttelsesforordningen, fortsat overholdes og at mulighederne ikke dækker fuldautomatiseret sagsbehandling.
IDA vil opfordre til, at det indskærpes i bemærkningerne, at medarbejderne skal have det relevante kompetenceniveau, når f.eks. en sagsbehandler benytter AI til beslutningsstøtte.

Overordnede bemærkninger

IDA anbefaler, at det indskærpes i bemærkningerne til lovforslaget, at det er nødvendigt, at de relevante kompetencer er tilstede både ved idriftsættelse og brug af AI systemer. Alle skal ikke kunne alt, men den enkelte medarbejder skal have den relevante forståelse af AI og det enkelte system. Med omnibussens ændringer af AI forordningen er artikel 4's krav til kompetencer ikke længere et krav, men en anbefaling. Når det kommer til behandling af sårbare data som persondata, er det imidlertid nødvendigt, at der er styr på både grundlæggende viden om AI-systemer, opmærksomhed på risikoen for fejl og bias samt påvirkning af den enkelte sagsbehandlers dømmekraft.

Specifikke bemærkninger

Jf. §1 finder IDA det rigtigt, at lovforslaget alene vil kunne anvendes som supplerende retsgrundlag for de behandlingsaktiviteter, som

myndigheder og organer vil foretage sig som led i samfundets interesse eller som led i deres varetagelse af myndighedsopgaver.
Jf. §3 finder IDA det rigtigt, at offentlige myndigheder og organer har mulighed for at udnytte fordelene ved de teknologiske muligheder, som AI-systemer giver. Det er dog vigtigt, at mulighederne begrænses til beslutningsstøtte og ikke fuldautomatiseret sagsbehandling, når det kommer til at omfatte personoplysninger.

Jf. §3 stk.2 vil IDA anbefale, at der udarbejdes en overordnet vejledning til brug for de enkelte ministres ressortområder, for at undgå alt for forskelligartede fortolkninger af brugen af AI-systemer til sagsbehandling, når formålet netop er at skabe klarere rammer.
Det bør også i bemærkningerne til §3, stk. 2 fremhæves, at en konsekvensvurdering af den registreredes rettigheder er et krav.

Jf. 2.1.2. s.15 er IDA enig i, at formålet med lovforslaget skal være at understøtte kvaliteten i opgavevaretagelsen og herudover kunne bidrage til at lette de administrative byrder for offentlige myndigheder. Det er væsentligt at være opmærksom på, at idriftsættelse af AI-systemer er en investering, der kræver både økonomi, medarbejderressourcer og øgede kompetencer. Flere eksempler har vist, at der også kan være tidsbesparelser, men at dette ikke nødvendigvis er tilfældet.

Jf. 2.1.2. s. 16 er IDA enig i, at hvis AI-systemet f.eks. skal anvendes over for særligt sårbare grupper af registrerede, bør det i særlig grad overvejes, hvordan der kan sikres det højest mulige beskyttelsesniveau for de registrerede.
IDA er også enig i, at lovforslaget ikke må påvirke de eksisterende rammer for videregivelse af personoplysninger blandt offentlige myndigheder og organer, ligesom anonymiserede personoplysninger jf. databeskyttelsesreglerne, ikke skal være omfattet af dette lovforslag.

Jf. 2.1.2. s. 17-18 kan IDA bakke op forslagets definition af begrebet "beslutningsstøtte", da det stemmer fint overens med den definition, der benyttes i standardiseringssammenhæng, herunder til de harmoniserede standarder vedr. AI.[1]
Her defineres beslutningsstøtte som "*automatisering af en beslutning eller levering af information, som et menneske kan benytte til at træffe en beslutning*".

[1] Se f.eks. DA/PAS 2500-2:2020 "Kunstig intelligens Del 2: Beslutningsstøttende anvendelse i offentlig sektor" www.ds.dk

Det er IDAs opfattelse, at lovforslaget dækker *"levering af information, som et menneske kan benytte til at træffe en beslutning*."

Man opererer i standardisering med tre grader af menneskelig inddragelse i beslutninger:
1. Menneskeinddragende beslutningsstøtte, der kræver menneskelig inddragelse, fx ved at levere dele af datagrundlaget for beslutningen eller som ansvarlig for at udføre beslutningen.
2. menneskemonitorereret beslutningsstøtte, der opererer uafhængigt af mennesker, men under menneskelig monitorering med intervention, når det er nødvendigt.
3. menneskeuafhængig beslutningsstøtte, der opererer uden menneskelig inddragelse.
Det er IDAs opfattelse, at lovforslaget dækker trin 1:
Menneskeinddragende beslutningsstøtte, der kræver menneskelig inddragelse, fx ved at levere dele af datagrundlaget for beslutningen eller som ansvarlig for at udføre beslutningen.

Jf. 2.2.1.1. s. 20 kan IDA bakke op om at myndighederne og organerne bør alene anvende de personoplysninger, der er nødvendige, tilstrækkelige og relevante for at kunne udvikle AI-systemet til at kunne udføre den tiltænkte opgave. Dataminimering er essentielt, når det kommer til at beskytte persondata.

Jf. 2.2.2.1. s. 27 og 2.2.2.2. s. 30 kan IDA bakke op om, at lovforslaget ikke vil fungere som en hjemmel til at behandle nye eller yderligere personoplysninger.

Jf. 2.2.2.3. s. 33 kan IDA bakke op om, at en mulig fremtidig udvikling af AI systemer ikke vil kunne anses som et hensyn til en videre eller forlænget opbevaring af personoplysninger, ud over hvad der i øvrigt er administrativt behov for og at myndigheder og organer ikke vil have mulighed for at genindhente personoplysninger fra et offentligt arkiv.

Med venlig hilsen

Grit Munk
Fagpolitisk chef digitalisering
IDA

INSTITUT FOR MENNESKE RETTIGHEDER

Wilders Plads 8K
1403 København K
Telefon 3269 8888
Mobil +45 91325706
sask@humanrights.dk
menneskeret.dk

Dok. nr. 26/01888-3

12. oktober 2026

Digitaliseringsstyrelsen
Landgreven 4
1017 København K

Sendt til jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk, og kahevi@digst.dk

Høringssvar over forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Digitaliseringsstyrelsen har ved e-mail af 14. september 2026 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Instituttet har bemærkninger til lovudkastet.

1. Sammenfatning

Det foreslås med lovudkastet, at der etableres en generel databeskyttelsesretlig hjemmel til at udvikle og anvende kunstig intelligens (AI)-systemer ved behandling af personoplysninger som led i deres opgavevaretagelse.

Lovudkastet vil indebære, at et stort omfang af offentlige myndigheder og organer vil tildeles en generel hjemmel til behandling af borgeres personoplysninger til udvikling og anvendelse af AI-systemer, herunder til profilering af borgere. Det vil efter instituttets opfattelse udgøre et indgreb i Den Europæiske Menneskerettighedskonvention (EMRK) artikel 8 og EU's Charter om Grundlæggende Rettigheder (EUC) artikel 7 og 8.

Instituttet antager, at lovudkastet forfølger et legitimt formål om landets økonomiske velfærd ved at forbedre og effektivisere brugen af samfundets ressourcer, hvor det er mest hensigtsmæssigt, og for at sikre beskyttelsen af andres ret og frihed, ved for eksempel at kunne identificere beskyttelseshensyn til borgere i myndigheders sagsbehandling og målrette indsatser mod disse.

Lovudkastet rejser imidlertid et centralt spørgsmål om, hvorvidt den foreslåede hjemmel kan anses for nødvendig i et demokratisk samfund, navnlig om det er tilstrækkeligt klart og proportionelt med det forfulgte formål.

Instituttet vurderer hertil, at brugen af AI indebærer en risiko for såkaldt "automatiseringsbias", hvor der er risiko for, at medarbejdere har for høj tillid til automatiserede beslutningssystemer, og – uden at være opmærksomme på det – eksempelvis laver hurtigere, mindre grundige vurderinger af en opgave, end de ellers ville, eller tillægger løsningens vurdering større betydning. Det udgør en yderligere risiko for uberettigede indgreb i borgerens rettigheder.

Lovudkastet rejser derudover spørgsmål om forbuddet mod diskrimination. Der er ifølge instituttet risiko for, at den foreslåede ordning kan medføre, at myndigheder ved udvikling og anvendelse af AI-systemer foretager ulovlig forskelsbehandling.

Lovudkastet rejser desuden spørgsmål om retten til effektive retsmidler. Myndighederne bør derfor sikre, at brugen af AI-systemer er tilstrækkeligt tilgængeligt og forståeligt for de personer, hvis rettigheder berøres, således at det er muligt at rejse eventuelle indsigelser om rettighedskrænkelser.

Herudover finder instituttet anledning til at fremsætte nogle generelle betragtninger om det offentliges brug af AI. Instituttet ville finde det formålstjenligt, at regeringen sikrer et generelt, tværgående overblik over udviklingen og anvendelsen af AI i det offentlige, herunder for at monitorere den samlede anvendelse af AI med betydning for borgernes menneskerettigheder.

På den baggrund anbefaler Institut for Menneskerettigheder:

- at Digitaliseringsstyrelsen sikrer, at – og beskriver hvordan – kravet til klarhed og proportionalitet i EMRK artikel 8 og EUC artikel 7 og 8 sikres opfyldt i praksis hos de konkrete myndigheder, herunder at formålet ikke kan opnås ved mindre indgribende foranstaltninger, såsom etablering af hjemlen alene for de myndigheder, hvor der er vurderet et konkret behov, der står mål med indgrebets karakter,
- at Digitaliseringsstyrelsen indarbejder et krav i lovudkastet om, at myndigheder skal sikre relevante procedurer såsom dokumentation, gennemsigtighed og ansvar ved brug af AI-systemer for at adressere risici for bias og diskrimination,
- at Digitaliseringsstyrelsen indarbejder et krav om, at myndigheder gennemfører en menneskeretlig konsekvensanalyse forud for ibrugtagning af et AI-system,
- at det præciseres i lovudkastet, hvornår der kan ske fravigelse fra rettighederne i databeskyttelsesreglerne samt hvilke materielle og processuelle garantier, der skal være opfyldt, og
- at Digitaliseringsstyrelsen indarbejder et krav i lovudkastet om, at der efter to år gennemføres en kortlægning og evaluering af hjemlens faktiske anvendelse i praksis, herunder med opgørelse af i hvilket omfang og på hvilken måde hjemlen har været anvendt til systemer, der reducerer borgernes menneskeretlige krav på privatliv, i hvilken udstrækning myndighederne har identificeret og forebygget risiko for bias og diskrimination samt i hvilket omfang den foreslåede hjemmel til at gøre undtagelser til borgernes rettigheder efter databeskyttelsesforordningen, har været udnyttet. Anbefalingen kan forudsætte, at der allerede ved loven indføres krav til dokumentation af disse forhold.

2. Lovudkastets indhold

Med lovudkastet foreslås etableringen af en generel databeskyttelsesretlig hjemmel til at udvikle og anvende AI-systemer ved behandling af personoplysninger som led i deres opgavevaretagelse.

Det vil indebære, at offentlige myndigheder og organer vil kunne behandle personoplysninger ved anvendelse af kunstig intelligens i form af AI-systemer, herunder til beslutningsstøtte, for eksempel i forbindelse med evaluering af bestemte personlige forhold vedrørende en borger (profilering).

Lovudkastets anvendelsesområde fortolkes bredt og omfatter samtlige offentlige myndigheder og organer, der varetager opgaver i samfundets interesse.

Anvendelsesområdet er afgrænset til de personoplysninger, som myndigheder i forvejen lovligt behandler – bl.a. personoplysninger indsamlet til andre formål – men vil ikke kunne bruges til hverken behandling af nye oplysninger, med henblik på at træffe fuldautomatiske afgørelser eller til videregivelse til andre myndigheder. Hjemlen vil give mulighed for at behandle følsomme personoplysninger og personoplysninger om straffedomme og lovovertrædelser, men lægger i den forbindelse op til, at ressortministeren vil have mulighed for at fastsætte yderligere foranstaltninger for beskyttelse af den registreredes rettigheder og interesser.

Derudover foreslås det i lovudkastet at etablere en mulighed for, at ressortministre og Domstolsstyrelsen ved bekendtgørelse kan vælge at etablere undtagelser til en række af bestemmelserne i databeskyttelsesforordningen, hvis betingelserne herfor efter databeskyttelsesreglerne er opfyldt. Det vurderes bl.a. nødvendigt af hensyn til myndigheder og organerne.

3. Menneskeretten

Lovudkastet giver anledning til overvejelser i forhold til EUC og EMRK.

Det vedrører navnlig EUC artikel 7 (respekt for privatliv og familieliv), artikel 8 (beskyttelse af personoplysninger), artikel 21 (ikke-forskelsbehandling) og artikel 47 (adgang til effektive retsmidler og til en upartisk domstol) samt EMRK artikel 8 (retten til privat- og familieliv), artikel 13 (adgang til effektive retsmidler) og artikel 14 (forbud mod diskriminering).[1]

Det følger af EUC artikel 7, at enhver har ret til respekt for sit privatliv, der indholdsmæssigt svarer til EMRK artikel 8. Det følger af EUC artikel 8, at enhver har

[1] Det følger af EUC artikel 51, stk. 1, at EUC finder anvendelse, når medlemsstater gennemfører EU-retten. I lovudkastet er der tale om etablering af et supplerende retsgrundlag under databeskyttelsesforordningen, jf. lovudkastets afsnit 3, s. 43 ff., hvorfor det forudsættes, at der er tale om gennemførelse af EU-retten.

ret til beskyttelse af personoplysninger.[2] Personoplysninger efter EUC artikel 7 og 8 dækker over enhver form for information om en identificeret eller identificerbar person.[3]

Efter EMRK artikel 8, stk. 1, har enhver ret til respekt for sit privatliv. Privatliv skal forstås bredt og omfatter bl.a. personoplysninger, information om personers private forhold og identitet, myndigheders lagring af data, der har forbindelse til enkeltpersoners privatliv, offentligt tilgængelige oplysninger, når myndigheder indsamler og opbevarer disse systematisk samt myndigheders behandling af data vedrørende bestemte individer på en måde eller i et omfang, der går ud over, hvad man kan forvente ved en sådan brug.[4]

Det følger af EUC artikel 52, stk. 3, at forhold der nyder tilsvarende beskyttelse efter EUC og EMRK, har samme betydning og rækkevidde, hvilket bl.a. er tilfældet for EUC artikel 7 og EMRK artikel 8.[5]

Det følger af EMRK artikel 8, stk. 2, og EUC artikel 52, at det er muligt at retfærdiggøre et indgreb i EMRK artikel 8 og EUC artikel 7 og 8, når indgrebet er foreskrevet ved lov, varetager et af de opregnede legitime formål og er nødvendig i et demokratisk samfund for at opnå det legitime formål. Stater tillades en vis skønsmargin i den forbindelse, men omfanget afhænger af karakteren af rettigheden, der gøres indgreb i, rettighedens betydning for individet og indgrebets intensitet, karakteren af de aktiviteter, der gøres indgreb i, og karakteren af det anerkendelsesværdige formål, der forfølges.[6]

Det indebærer bl.a., at en lov der giver mulighed for indgreb i disse rettigheder, skal være tilstrækkeligt klar til, at borgere kan forudsige konsekvenserne heraf og indrette sig efter det. Kravene til klarheden i loven afhænger af indholdet af reguleringen, det område der reguleres, og antallet og karakteren af de private, som berøres af reguleringen. Kravet udelukker ikke, at myndigheder kan overlades et skøn, men i sådanne tilfælde skal der sikres klarhed over omfanget og graden af

---

[2] Beskyttelsen i EUC artikel 8 udgør en selvstændig beskyttelse af personoplysninger, men i praksis anses bestemmelsen for at være nært beslægtet med EUC artikel 7.

[3] Se EUD's udtalelse 1/15 af 26. juli 2017, pr. 122, dom af 24. november 2011, *ASNEF*, forenede sager C-468/10 og C-469/10, pr. 41, samt Christoffersen, J., m.fl., *EU's Charter om Grundlæggende Rettigheder* (2. udgave, DJØF 2018), s. 126.

[4] Se bl.a. Amann mod Schweiz, dom af 16. februar 2000, pr. 65, Gaskin mod Storbritannien, dom af 7. juli 1989, pr. 38 ff., Leander mod Sverige, dom af 26. marts 1987, pr. 48, Rotaru mod Rumænien, dom af 4. maj 2000, pr. 43-44 og Satakunnan Markkinaporssi Oy og Satamedia mod Finland, dom af 27. juni 2017, pr. 136.

[5] Det betyder, at beskyttelsesområdet og indgrebet i disse rettigheder skal fastlægges ud fra praksis hos både EU-domstolen og Den Europæiske Menneskerettighedsdomstol (Menneskeretsdomstolen). EUC kan dog sikre et højere beskyttelsesniveau end EMRK. Det har man i nogen grad set for indgreb i beskyttelsen af personoplysninger, hvor EU-domstolen på en række områder har stillet større krav til indgrebets lovlighed, hvilket adskiller sig fra indgreb i andre rettigheder, hvor stater normalt efterlades et bredere skøn, jf. bl.a. Christoffersen, J., m.fl., EU's Charter om Grundlæggende Rettigheder (2. udgave, DJØF 2018), s. 578-587 og *Tele2 Sverige og Watson m.fl*, forenede sager C-203/15 og C-698/15, pr. 96.

[6] Connors mod Storbritannien, dom af 27. maj 2004, pr. 82.

myndighedernes skøn samt tilstrækkelig beskyttelse mod vilkårlige indgreb, navnlig når personoplysninger udsættes for automatiseret behandling.[7]

Menneskeretsdomstolen har i flere tilfælde forholdt sig til spørgsmålet om indgreb i retten til privatliv i forbindelse med staters brug af ny teknologi.

Domstolen har i en sag om myndighedernes anvendelse og opbevaring af fingeraftryk, biologiske prøver og DNA-profiler i retshåndhævelses øjemed udtalt, at fordelene ved brug af moderne videnskabelige metoder skal forholde sig nøje til privatlivets fred, og at stater, der er pionerer i udviklingen af nye teknologier, bærer et særligt ansvar for at ramme den rette balance heri. Domstolen udtalte bl.a. i sagen, at det er relevant for indgreb i privatlivets fred at forholde sig til den mulige fremtidige brug af private oplysninger, og at den hastige udvikling på området for genetik og informationsteknologi ikke kan udelukke, at privatlivets fred i fremtiden kan blive alvorligt påvirket på nye måder, eller på måder der ikke kan forudses i dag.[8]

Det følger af EMRK artikel 13, at enhver, der får krænket de i EMRK anerkendte rettigheder og friheder, skal have adgang til effektiv oprejsning for en national myndighed, uanset om krænkelsen er begået af personer, der handler på embeds vegne. En lignende beskyttelse findes i EUC artikel 47. Det følger af EMRK artikel 14, at nydelsen af de i EMRK anerkendte rettigheder og friheder skal sikres uden forskel på grund af køn, race, farve, sprog, religion, politisk eller anden overbevisning, national eller social oprindelse, tilhørighed til et nationalt mindretal, formueforhold, fødsel eller ethvert andet forhold. En lignende beskyttelse findes i EUC artikel 21.

Europarådet vedtog på et ministerrådsmøde den 17. maj 2024 Europarådets rammekonvention om kunstig intelligens og menneskerettigheder, demokrati og retsstatsprincippet. Konventionen fastsætter en række grundlæggende principper såsom ikke-forskelsbehandling, gennemsigtighed, tilsyn samt ansvarlighed. Herudover stiller konventionen bl.a. krav om at dokumentere brug af AI og at gøre disse oplysninger tilgængelige for berørte personer, så de er i stand til at påklage brugen til relevante myndigheder samt at gennemføre menneskeretlige konsekvensanalyser.[9]

Europarådets ekspertkomité for menneskerettigheder (CDDH), der rådgiver Europarådets ministerkomité, udgav i april 2026 en håndbog om menneskerettigheder og AI. I håndbogen fremhæves, at brugen af AI rummer en

---

[7] Se bl.a. Karacsony og andre mod Ungarn, dom af 17. maj 2026, pr. 123-125, Catt mod Storbritannien, dom af 24. januar 2019, pr. 94, Vukota-Bojic mod Schweiz, dom af 18. oktober 2016, pr. 66 ff., dom af 8. april 2014, *Digital Rights Ireland m.fl.*, forenede sager C-293/12 og C-594/12, pr. 54, og S &. Marper mod Storbritannien, dom af 4. december 2008, pr. 103.

[8] S &. Marper mod Storbritannien, dom af 4. december 2008, pr. 112.

[9] Europarådets rammekonvention om kunstig intelligens og menneskerettigheder, demokrati og retsstatsprincippet (Europarådets rammekonvention om kunstig intelligens og menneskerettigheder, demokrati og retsstatsprincippet). Rammekonventionen er udarbejdet af 46 medlemsstater, og er bl.a. blev tiltrådt af EU på vegne af medlemsstaterne.

række tværgående risici, navnlig i forhold til ikke-forskelsbehandling og lighed, beskyttelsen af personoplysninger og privatliv samt muligheden for at anfægte AI-baserede beslutninger tilstrækkeligt.[10]

4. Instituttets bemærkninger

4.1. Instituttets vurdering af lovudkastet

Institut for Menneskerettigheder har den 7. april 2026 afgivet høringssvar til det tidligere lovudkast, der blev sendt i høring den 12. februar 2026.[11]

Lovudkastet rejser dog fortsat en række menneskeretlige overvejelser.

Det fremsatte lovudkast rejser væsentlige spørgsmål om retten til privatliv og retten til beskyttelse af personoplysninger. Instituttet bemærker, at lovudkastet ikke indeholder nogen beskrivelse af forholdet til EMRK.

Risiko for vilkårlighed og behov for menneskeretlig vurdering

Lovudkastet vil indebære, at et stort omfang af offentlige myndigheder og organer vil tildeles en generel hjemmel til behandling af borgeres personoplysninger til udvikling og anvendelse af AI-systemer, herunder til profilering af borgere. Det vil efter instituttets opfattelse udgøre et indgreb i EMRK artikel 8 og EUC artikel 7 og 8.

Det fremgår af lovudkastet, at formålet er at understøtte kvaliteten i myndighedernes opgavevaretagelse og lette de administrative byrder for offentlige myndigheder og organer.

Instituttet antager, at lovudkastet forfølger et legitimt formål om landets økonomiske velfærd ved at forbedre og effektivisere brugen af samfundets ressourcer, hvor det er mest hensigtsmæssigt, og for at sikre beskyttelsen af andres ret og frihed, ved for eksempel at kunne identificere beskyttelseshensyn til borgere i myndigheders sagsbehandling og målrette indsatser mod disse.

Lovudkastet rejser imidlertid et centralt spørgsmål om, hvorvidt den foreslåede hjemmel kan anses for nødvendig i et demokratisk samfund, navnlig om det er tilstrækkeligt klart og proportionelt med det forfulgte formål.

Instituttet noterer, at den foreslåede hjemmel bl.a. er afgrænset til behandling af personoplysninger inden for databeskyttelsesforordningen, og til personoplysninger som myndigheder allerede behandler efter et lovligt formål.

Omvendt medfører lovudkastets brede anvendelsesområde en risiko for vilkårlig retsudøvelse.

---

[10] Steering Committee for Human Rights (CDDH), Europarådets menneskerettighedskomité under Ministerkomitéen,, april 2026 (48802b5bf2), s. 22.

Hjemlen vil omfatte et meget stort omfang af myndigheder og organer uden hensyntagen til den enkelte myndigheds konkrete behov, kapacitet og vidensniveau samt kompetence til at sikre tilstrækkelig beskyttelse af oplysningerne og sikker drift af AI-systemet.

Hjemlen omfatter desuden et meget stort omfang af personoplysninger, herunder følsomme personoplysninger med et skærpet beskyttelsesbehov, uden krav om, at der fastsættes beskyttelsesforanstaltninger. Det indebærer en risiko for, at den samlede mængde af følsomme personoplysninger kan give meget detaljerede eller sågar helt nye profiler af borgere. Det indebærer desuden risiko for særligt intensive indgreb i kernen af privatlivets fred og beskyttelsen af personoplysninger – også i tilfælde, hvor den rettighed, der gøres indgreb i, kan have et større beskyttelsesbehov, eller i situationer hvor borgeren ikke har en individuel interesse i myndighedens anvendelse af AI-systemer.

Det fremgår af lovudkastet, at AI-systemer i mange tilfælde er opbygget ved komplekse datastrukturer, hvor oplysninger fra mange registrerede indgår i træningsdatasæt, og hvor det ikke altid vil være muligt at udskille de registreredes personoplysninger fra modelparametrene. Derved kan AI-systemernes funktionsmåde gøre det vanskeligt, eller i visse tilfælde sågar umuligt, for myndighederne og organerne at håndtere de registreredes rettigheder, når først personoplysningerne er indlejret i et AI-system.[12] Dette kan yderligere kompliceres, hvis myndigheder indkøber AI-systemer med begrænset gennemsigtighed hos eksterne leverandør.

Som eksempel på lovudkastets mulige rækkevidde kan nævnes, at told- og skatteforvaltningen siden 2021 har haft hjemmel til at behandle og samkøre alle nødvendige oplysninger fra offentligt tilgængelige kilder, herunder sociale medier, offentlige registre og hjemmesider.[13] Skatteforvaltningens borger- og retssikkerhedschef har af hensyn til den teknologiske udvikling anbefalet skatteforvaltningen om at danne sig et overblik over metoderne til indsamling af disse oplysninger og behovet for at udarbejde yderligere retningslinjer herom.[14]

Eftersom lovudkastets ordning er afgrænset til de personoplysninger, som myndigheden i forvejen lovligt behandler, vil der i skatteforvaltningens tilfælde kunne udvikles og anvendes et AI-system, der trænes på en omfattende mængde offentligt tilgængelige oplysninger om borgere. Dette kan føre til en profilering af borgere til brug for forvaltningens arbejde med eksempelvis inddrivelse af offentlig gæld eller afgørelse om efteropkrævning. Hvis disse offentligt tilgængelige oplysninger ikke er ajourført eller upræcise, kan det medføre væsentlige negative konsekvenser for borgeren uden indsigt heri.

---

[12] Lovudkastet, s. 40 og 77.
[13] L 73 som vedtaget ved lov nr. 2612 af 28. december 2021
[14] Skatteforvaltningens borger- og retssikkerhedschefs notat-om-skatteforvaltningens-indsamling-behandling-og-brug-af.pdf af april 2024, s. 19

En vurdering af, om skatteforvaltningens beslutning om at behandle oplysninger ved brug af AI-systemer er i overensstemmelse med menneskeretten, vil med lovudkastet i ovenstående eksempel blive overladt til skattemyndighederne.

Det gør det meget svært for borgerne at forudsige konsekvenserne af loven, og medfører risiko for uigennemsigtige AI-systemer, hvor det er svært – eller sågar umuligt – reelt at forudsige og håndtere konsekvenserne af myndighedernes behandling af personoplysninger ved udvikling og anvendelse af AI-systemer. Det vil både gøre det vanskeligt for borgerne at få indsigt i, hvordan deres oplysninger behandles og med hvilken risiko samt gøre det svært for borgeren at indrette sig efter disse risici og at gøre indsigelser mod behandlingen.

Instituttet anbefaler fortsat – som i sit høringssvar af 7. april 2026 – at der som det klare udgangspunkt stilles krav om, at myndigheder udarbejder og offentliggør menneskeretlige konsekvensanalyser, før nye AI-systemer tages i brug og anvendes. Instituttet anbefaler fortsat også, at det præciseres yderligere i lovudkastet, hvornår der kan ske fravigelse fra rettighederne i databeskyttelsesreglerne samt hvilke materielle og processuelle garantier, der skal være opfyldt.

Risiko ved automatiseret beslutningsstøtte
Instituttet finder det positivt, at man i lovudkastet har afgrænset og præciseret begrebet "beslutningsstøtte" yderligere, som instituttet bl.a. anbefalede til det tidligere lovudkast. Instituttet bemærker dog, at der fortsat henvises til, at fremtidig praksis vil bidrage til at præcisere, hvilken grad af menneskelig involvering der kræves, før der er tale om "beslutningsstøtte".

Det fremgår af lovudkastet, at afgrænsningen mellem fuldautomatiske afgørelser og beslutningsstøtte afhænger af omfanget af den menneskelige involvering. Denne afklaring kan understøttes af procedurer til at identificere, hvem der har beslutningskompetence ved brug af AI-systemer, hvordan afvigelser fra systemets anbefalinger håndteres samt sikre relevant logning og anvendelse af systemet. Det fremgår imidlertid af lovforslaget, at der ikke stilles krav om sådanne procedurer.

Brugen af AI indebærer en risiko for såkaldt "automatiseringsbias", hvor der er risiko for, at medarbejdere har for høj tillid til automatiserede beslutningssystemer, og – uden at være opmærksomme på det – eksempelvis laver hurtigere, mindre grundige vurderinger af en opgave, end de ellers ville, eller tillægger løsningens vurdering større betydning. Det udgør en yderligere risiko for uberettigede indgreb i borgerens rettigheder. Uanset at det fremgår af lovforslaget, at brugen af AI begrænses til "beslutningsstøtte", kan der således være risiko for, at AI utilsigtet bruges anderledes. Medarbejdernes kompetenceniveau, herunder indsigt i AI-systemet samt ressourcer og arbejdsmængde vil på samme måde kunne være væsentlig for realiteten af medarbejderens involvering.

Risiko for forskelsbehandling som følge af bias i AI-systemer
Lovudkastet rejser derudover spørgsmål om forbuddet mod diskrimination.

Det fremgår af lovudkastet, at der foreligger en risiko for, at lovudkastet kan medføre potentielle negative ligestillingsmæssige konsekvenser. Herom fremgår at ved at give offentlige myndigheder og organer en bred adgang til at anvende AI-systemer til at understøtte opgavevaretagelsen efter anden lovgivning, vil risikoen for, at borgere udsættes for forskelsbehandling på baggrund af de iboende bias i AI-systemerne, være til stede. Det fremgår imidlertid ikke af lovudkastet, hvordan disse risici vil adresseres som følge af den konkret foreslåede ordning.

Der ses således i lovudkastet redegjort dels for konkrete, iboende risici for bias i de AI-systemer, der gives en bred hjemmel til udvikling og anvendelse af på tværs af en bred række myndigheder, dels for at disse systemers funktionsmåde kan gøre det vanskeligt og i visse tilfælde umuligt for myndighederne at håndtere de registreredes rettigheder, når oplysningerne er indlejret i et AI-system. Dette uden at man i lovudkastet modsvarer disse risici med konkrete beskyttelsesforanstaltninger, herunder ved at stille krav om dokumentation.

Det udgør ifølge instituttets vurdering en risiko for, at den foreslåede ordning kan medføre, at myndigheder ved udvikling og anvendelse af AI-systemer foretager ulovlig forskelsbehandling.

Adgang til effektive retsmidler
Enhver, der har en rimelig begrundet påstand om, at deres rettigheder er blevet krænket, skal have adgang til effektive retsmidler. Det er også en del af de processuelle forpligtelser, der følger af for eksempel retten til privatliv.

Brugen af AI-systemer medfører en betydelig risiko for manglende gennemsigtighed og indsigt i myndigheders brug af disse systemers og deres tekniske kompleksitet, deres afhængighed af enorme datasæt og de forskellige aktører i forsyningskæden. Enkeltpersoner kan derfor mangle den viden eller adgang til de oplysninger, der er nødvendige for at identificere eventuelle rettighedskrænkelser eller for at indrette sig efter disse risici. Der er også risiko for en grundlæggende mangel på kendskab til omfanget af indgrebet i deres rettigheder, ligesom det kan være svært at forstå de underliggende beslutningsprocesser, herunder graden af menneskelig involvering.

Myndighederne bør derfor sikre, at brugen af AI-systemer er tilstrækkeligt tilgængeligt og forståeligt for de personer, hvis rettigheder berøres, således at det er muligt at rejse eventuelle indsigelser om rettighedskrænkelser. Instituttet bemærker, at lovudkastet ikke stiller specifikke krav til, om og hvordan offentlige myndigheder skal oplyse berørte borgere om brugen af deres oplysninger i AI-systemer og i eventuelle afgørelser rettet mod dem.

4.2 Generelle betragtninger om kunstig intelligens
Institut for Menneskerettigheder finder derudover anledning til at fremsætte nogle generelle betragtninger om det offentliges brug af AI.

AI finder stor udbredelse i samfundet i både det offentlige og private rum med stor hast, hvilket både rummer potentialer og risici. Danmark er et digitalt foregangsland, og derfor er der også et stort fokus på at bruge AI til at opnå fordele i forvaltningen såsom øget effektivisering. I regeringsgrundlagets afsnit om AI lægges der bl.a. op til at accelerere udnyttelsen af AI i den offentlige sektor ved strategisk satsning på løsninger med stort innovations- og skaleringspotentiale, hvorfor der tages initiativ til etableringen af en AI-accelerationsfond for kunstig intelligens, der skal sætte turbo på udrulningen af AI. Der lægges desuden op til at fremme projekter med AI i kommuner og regioner med klare potentialer for innovation og skalering samt at fortsætte udrulningen af storskalaprojekter i samarbejde med KL og Danske Regioner i regi af Den Digitale Taskforce for Kunstig Intelligens.[15]

Den brede samfundsdebat om hastigheden i udviklingen og anvendelsen af AI har den seneste tid skærpet fokusset på risici forbundet med accelerationen af AI[16]

Instituttet bemærker på den baggrund, at den aktuelle status for udviklingen og anvendelsen af kunstig intelligens rejser en række spørgsmål om hastigheden i udviklingen og brugen af AI set i lyset af de risici og konsekvenser, som den seneste tids eksempler har vist. Dette skal ses i sammenhæng med udrulningen af AI i det offentlige, navnlig når der ikke tages stilling til risici forbundet med de konkret valgte AI-systemer som eksempelvis ovennævnte. Instituttet vurderer, at det kan få betydning for den menneskeretlige situation i Danmark fremadrettet, men at det netop ikke er muligt at vurdere dette i forbindelse med så bred en hjemmel som den foreslåede.

I den forbindelse ville instituttet finde det formålstjenligt, at regeringen sikrer et generelt, tværgående overblik over udviklingen og anvendelsen af AI i det

---

[15] Regeringen, det politiske grundlag for firkløverregeringen af juni 2026 (det-politiske-grundlag-for-firkloeverregeringen.pdf), s. 60.

[16] Som konkrete eksempler kan nævnes, at AI-modeller fra en af de førende udviklere af AI, OpenAI (der bl.a. står bag sprogmodellen ChatGPT), i juni 2026 uden menneskelig indblanding tilgik den australske regerings hjemmesider uden autorisation. I en anden hændelse offentligt kendt som "Hugging Face-skandalen" i juli 2026 omgik OpenAI's modeller på egen hånd sikkerhedsforanstaltninger for at tilgå internettet, hvorefter de hackede sig ind i et andet firma. Modellerne havde i strid med formålet kommunikeret via uautoriserede kanaler, herunder med hinanden, udnyttet sårbarheder i teknisk infrastruktur og fået adgang til internettet. OpenAI beskrev selv hændelsen som et "advarselsskud" til resten af verden om, hvad meget stærke og sofistikerede AI-agenter kan udføre. Se bl.a. OpenAI, "The Hugging Face incident and the road ahead" (The Hugging Face incident and the road ahead | OpenAI) (besøgt den 6. Oktober 2026).

Bekymringer forbundet med AI er i stigende grad også begyndt at blive udtrykt af førende ledere inden for den branche, hvor AI udvikles. I august 2026 udtalte Bill Gates bl.a., at man nu har overskredet tærsklerne, hvad angår AI's biologiske, cybermæssige og psykosociale evner, dens evne til at ødelægge arbejdsmarkedet og endda manglen på kontrol. I september 2026 skrev direktøren for en af de andre førende udviklere af AI, Anthropic, at de seneste måneder havde overbevist ham om, at tilstrækkelig håndtering af risici forbundet med AI kræver endnu større forsigtighed, herunder at man bør sænke tempoet, hvormed AI-modellernes forbedres. Se bl.a. Mat Honan, "Bill Gates says we've passed AI's danger thresholds. Now what?" (Bill Gates says we've passed AI's danger thresholds. Now what? | MIT Technology Review) (besøgt den 6. oktober 2026), Dario Amodei, "We Must Pace the Frontier" (Dario Amodei — We Must Pace the Frontier) (besøgt den 6. oktober 2026)

offentlige, herunder for at monitorere den samlede anvendelse af AI med betydning for borgernes menneskerettigheder, jf. ovenfor.

På den baggrund anbefaler Institut for Menneskerettigheder:

- at Digitaliseringsstyrelsen sikrer, at – og beskriver hvordan – kravet til klarhed og proportionalitet i EMRK artikel 8 og EUC artikel 7 og 8 sikres opfyldt i praksis hos de konkrete myndigheder, herunder at formålet ikke kan opnås ved mindre indgribende foranstaltninger, såsom etablering af hjemlen alene for de myndigheder, hvor der er vurderet et konkret behov, der står mål med indgrebets karakter,
- at Digitaliseringsstyrelsen indarbejder et krav i lovudkastet om, at myndigheder skal sikre relevante procedurer såsom dokumentation, gennemsigtighed og ansvar ved brug af AI-systemer for at adressere risici for bias og diskrimination,
- at Digitaliseringsstyrelsen indarbejder et krav om, at myndigheder gennemfører en menneskeretlig konsekvensanalyse forud for ibrugtagning af et AI-system,
- at det præciseres i lovudkastet, hvornår der kan ske fravigelse fra rettighederne i databeskyttelsesreglerne samt hvilke materielle og processuelle garantier, der skal være opfyldt, og
- at Digitaliseringsstyrelsen indarbejder et krav i lovudkastet om, at der efter to år gennemføres en kortlægning og evaluering af hjemlens faktiske anvendelse i praksis, herunder med opgørelse af i hvilket omfang og på hvilken måde hjemlen har været anvendt til systemer, der reducerer borgernes menneskeretlige krav på privatliv, i hvilken udstrækning myndighederne har identificeret og forebygget risiko for bias og diskrimination samt i hvilket omfang den foreslåede hjemmel til at gøre undtagelser til borgernes rettigheder efter databeskyttelsesforordningen, har været udnyttet. Anbefalingen kan forudsætte, at der allerede ved loven indføres krav til dokumentation af disse forhold.

Med venlig hilsen

Johan Busse
National og juridisk chef

IT-Branchen
Langebrogade 4
1411 København K
Telefon: 60 15 23 30
Mail: itb@itb.dk

Til Digitaliseringsstyrelsen, att. Jonathan Meijer (jonmei@digst.dk) og Lea Marie Omdahl (leaomd@digst.dk), samt kahevi@digst.dk og emimol@digst.dk.

København, d. 9. oktober, 2026.

Høringssvar fra IT-Branchen vedrørende forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

IT-Branchen har modtaget forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven), og indsender hermed vores høringssvar.

IT-Branchen indsendte høringssvar på den første udgave af dette lovforslag (februar 2026), hvorfor der vil være et delvist overlap mellem de to høringssvar.

IT-Branchen er en selvstændig brancheorganisation der repræsenterer teknologivirksomheder i Danmark. Lovforslaget er højst aktuelt for vores medlemsvirksomheder, hvoraf en stor del af dem, er eksisterende leverandører af digitalisering, AI-løsninger, samt AI løsninger til det offentlige.

Opsummerende af væsentligste bemærkninger

IT-Branchen ser meget positivt på, at der etableres et fælles retsgrundlag og hjemmel for bred anvendelse og udvikling af AI ved behandling af personoplysninger i den offentlige forvaltning. Vi mener, at lovforslagets formål om at understøtte kvalitet og effektivitet i det offentlige igennem AI, er den rigtige vej at gå.

Vi ser også positivt på, at flere af de uklarheder som vi påpegede i høringssvaret til første forslag til denne lov (februar 2026), bl.a. uklarhed om hjemmel til profilering, uklarhed om forståelsen af beslutningsstøtte og relationen til sektorlovgivning, er uddybet og specificeret i dette lovforslag.

Lovforslaget lægger et stort ansvar for AI-området ud til de enkelte ressortområder/ministerier, særligt ift. ressortministerens mulighed for at lave undtagelser for den registreredes rettigheder, samt behandle persondata af særlig følsom karakter. Det kan der være både fordele og ulemper ved. Vi er bekymrede for, at hver minister eller ministerium laver sit eget unikke AI-regelsæt. Det kan betyde at digitaliseringen dels bliver meget fragmenteret og uens på tværs af samfundet. Derudover at ressortspecifikke særinteresser fx omkring undtagelser for den registreredes rettigheder, vil svække tilliden til den offentlige digitalisering.

Det er afgørende, at lovforslaget skaber et mere sammenhængende marked og mulighedsrum for udvikling og anvendelse af AI, og ikke – på trods af en generel hjemmel – skaber et uens og uklart marked, der samtidigt potentielt svækker tilliden til den offentlige forvaltning.

Generelle bemærkninger

Positivt med hjemmel til anvendelse af AI

IT-Branchen ser meget positivt på, at der etableres en generel hjemmel for anvendelse af AI ved behandling af personoplysninger i den offentlige forvaltning, herunder offentlige organer, samt at det nye forslag gør anvendelsesmulighederne, herunder beslutningsstøtte og profilering, endnu tydeligere. Både i forhold til træning og drift af AI-systemer. Det vil spare tid og ressourcer i den offentlige forvaltning ikke hver gang at skulle starte med at afklare hjemmelsspørgsmål og juridiske gråzoner. Noget som har bremset eller forsinket AI-projekter indtil nu.

Danmark har en højt digitaliseret offentlig sektor, og samtidigt et marked af it-leverandører, der er klar til at udvikle og anvende digitale løsninger til gavn for borgere, medarbejdere og samfundet. I lyset af Europas svækkede konkurrenceevne er det afgørende at ny lovgivning i Danmark, er med til at højne vores samlede konkurrenceevne. En entydige hjemmel til anvendelse og udvikling af AI, vil gøre det nemmere for både leverandører og offentlige myndigheder og organer at implementere og anvende AI-teknologi. Det vil samtidigt udbygge den danske styrkeposition indenfor offentlig digitalisering samt styrke mulighederne for, at danske tech-virksomheder kan levere AI-løsninger målrettet til den offentlige sektors behov. Vi vil dog opfordre til, at AI-loven ikke kommer til at stå alene, men at der fortsat vil være fokus på simplificering af regulering omkring AI i EU-regi.

Vores vurdering er, at lovhjemlen vil bidrage positivt til Danmarks konkurrenceevne, fordi it-leverandører i Danmark kan udvikle og implementere specialiserede AI-løsninger til den offentlige sektor i Danmark, som derefter kan eksporteres til andre lande. Selvom der med dette lovforslag kommer en bred lovhjemmel, så vil vi gøre opmærksom på, at der vil være brug for en omfattende vejledningsindsats for både borgere, offentlige myndigheder og virksomheder.

Ressortministrenes mulighedsrum bekymrer

Vores gennemgående bekymring ved lovforslaget er, at det giver ressortministrene vide beføjelser til fx at etablere undtagelser til en række bestemmelser i databeskyttelsesforordningen samt mulighed for at behandle særlige kategorier af personoplysninger.

Det er problematisk fordi digitalisering på et givent område kan blive knyttet til tilliden til det enkelte område og minister, og ikke den offentlige sektor som helhed. Vi har i Danmark høj tillid generelt til den offentlige, såvel som offentlige digitale løsninger. Den tillid, skal vi ikke sætte over styr.

Vi er bekymret for, at en ministers præferencer og politiske mål kan føre til, at anvendelse og udvikling af AI på forskellige ressortområderne bliver fragmenteret og uens. Ikke ud fra nøgterne risici og muligheder/begrænser ift. databeskyttelse mv., men ud fra den enkelte ministers politiske ønsker.

Efter dialog med Digitaliseringsstyrelsen forstår vi det således, at dette lovforslag gør det muligt for den enkelte ressortminister igennem bekendtgørelser at lave undtagelser af fx registreredes rettigheder, da disse ikke kan fastsættes bredt på tværs af ressortområder. Vi opfordrer til, at rammerne for AI blev fastsat mere centralt, fx med dette lovforslag, fremfor på ressortområderne. Vi foreslår også, at der indføres et forum for erfaringsudveksling eller 'checks and balances' så ressortministrene dels lærer af hinanden, samt at udvikling og anvendelse af AI implementeres

bredest muligt samt at anvendelsen af AI ikke bliver en politisk omskiftelig kampplads. Det har hverken borgere, samfund eller virksomheder gavn af.

Ikke at give hjemmel til automatiske afgørelser er kortsigtet

Det fremgår at lovforslaget ikke giver hjemmel til automatiske afgørelser. Det kan på nuværende tidspunkt være den rigtige position, men fremfor at afvise automatiske afgørelser fuldstændigt, så mener vi i IT-Branchen, at man i stedet skal se på mulighederne for automatiske afgørelser på ikke-følsomme og lav-risicifyldte områder. Herunder skal automatiske afgørelser være frivilligt, ligesom borgere eller virksomheder, der foretrækker manuel fremfor automatisk behandling af en sag, ikke må stilles ringere.

Det er vores vurdering, at en grad af automatisering af afgørelser, forventeligt bliver en del af fremtidens offentlige forvaltning. Derfor opfordrer IT-Branchen til, at regeringen allerede nu åbner dialogen op for og med involvering fra en bred skare af interessenter, herunder brancheforeninger, virksomheder, civilsamfund/borger, patient- og medlemsorganisationer samt forskning., om hvor og hvordan automatiske afgørelser eventuelt kan være en relevant mulighed og hvor vi som samfund ikke ønsker at automatiske afgørelser er del af den offentlige forvaltning i Danmark.

Helt generelt er det vigtigt for os som brancheforening, at de risici og konsekvenser for borgerne, som der nævnes i bemærkningerne, tages alvorligt, og der opstilles muligheder for check af, om et digitalt system – AI eller ej – har en bias overfor grupper af borgere. En højt digital offentlig sektor, og en stærk digital sektor, der kan udvikle løsninger til det offentlige, trives med en høj grad af tillid og transparens. Derfor er det vigtigt, at der tænkes i mitigerende handlinger overfor de risici, som fx AI i sagsbehandling indebærer.

Specifikke bemærkninger

IT-Branchen ser positivt på, at flere af de uklarheder som vi påpegede i høringssvaret til første forslag til denne lov (februar 2026), bl.a. uklarhed om hjemmel til profilering, uklarhed om forståelsen af beslutningsstøtte og relationen til sektorlovgivning, er uddybet og specificeret i dette lovforslag. Det ifølge vores forståelse følgende.

Uklarheder påpeget i tidligere høringssvar:

1) Lovforslagets forståelse af beslutningsstøtte:
    a. Dette er specificeret i bl.a. §2, samt fx side 17 og 18.

2) Uklart om lovforslaget giver hjemmel til anvendelse/udvikling af AI på historiske data (persondata indsamlet til et andet formål end anvendelse/udvikling af AI):
    a. Dette er specificeret bl.a. på side 33.

3) Uklart hvorvidt der er hjemmel til profilering i lovforslaget:
    a. Dette er specificeret flere steder i lovforslaget, samt i selve høringsbrevet.

4) Relation til sektorlovgivning, mere specifikt sektorspecifikke lovhjemler til anvendelse af AI
    a. Dette er specificeret bl.a. på side 15.

Uklarheder i lovforslaget

I lovforslaget eksisterer der følgende uklarheder som bør uddybes eller gøres klarere:

1) Uklarhed om offentlige myndigheder og organers muligheder for at dele data, herunder data fra offentlige arkiver
    a. Lovforslaget beskriver behandling af personoplysninger, også kan indebære videregivelse af data. Men, lovforslaget beskriver også, at offentlige myndigheder ikke må datadele, eller behandle, herunder samkøre nye personoplysninger (s. 27). Det kan derfor fra lovforslaget være uklart, hvor grænserne går for anvendelse eller træning af AI på offentlige myndigheders data? Efter dialog med Digitaliseringsstyrelsens forstår vi det således, at man som offentlig myndighed, kun må anvende AI på de data, som man i forvejen af lovlig adkomst til at behandle/opbevare. Dette bør tydeliggøres af lovforslaget. Lovforslaget beskriver også (s. 71), at offentlige myndigheder *ikke* må anvende data fra offentlige arkiver, hvis den offentlige myndighed ikke har disse data længere. Såfremt det ikke vil have en negativ påvirkning for de personer, om hvem der ligger data i offentlige arkiver, fx hvis den offentlige myndighed anonymiserer disse data, så ser vi i IT-Branchen at offentlige myndigheder *gerne* måtte anvende data til fx træning af AI-modeller.

2) Uklarhed om rammerne for videreudvikling og implementering af modeller kan fortolkes som datadeling af personoplysninger mellem myndigheder
    a. Vi forstår lovforslaget således, at AI modeller i sig selv ikke kan fortolkes som værende personoplysninger – uagtet at en model er trænet på personoplysninger. Derfor bør det være inden for rammen af dette lovforslag, at en leverandør, der har udviklet, trænet og/eller forbedret en model bl.a. med data og personoplysninger fra én myndighed (fx Kommune 1) gerne må sælge/videreudvikle denne model til en anden myndighed (fx Kommune 2), så længe at data ikke kan trækkes ud af modellen og at dette derfor ikke fortolkes som datadeling mellem myndigheder. Dette er der behov for bliver præciseret i lovforslaget.

3) Uklarhed om rammerne for samarbejdet mellem leverandør af AI-system som databehandler
    a. Det fremgår af lovforslagets bemærkninger (s. 29), at en offentlig myndighed selv kan udvikle eller få udviklet et AI-system. Da det i de fleste tilfælde vil være en privat leverandør der udvikler en AI-løsning, også selvom det er på/med data fra den offentlige myndighed, forstår vi det således at hjemlen også omfatter disse tilfælde. Det fremgår ikke eksplicit af lovforslaget og bør gøres tydeligere. Det er vigtigt at det er gennemsigtigt hvilke betingelser der gælder når en model, der er udviklet, trænet eller finjusteret på én myndigheds data, kan anvendes, tilpasses videreudvikles til gavn for andre myndigheder med deres data.

4) Uklarhed om forskellen på ”automatisk” og ”fuldautomatisk”
    a. Lovforslaget specificerer, at det ikke giver hjemmel til automatiske afgørelser, som bemærket ovenfor. Dog er det uklart igennem lovforslaget, hvad forskellen fx er på ”fuldautomatiske afgørelser” og ”automatisk individuelle afgørelser”? Samt, om ”automatisk behandling” vil være det samme som potentiel ”fuldautomatisk behandling”? Derudover nævnes automatiske afgørelser ofte i relation til fx retten til ikke at blive udsat for automatiske afgørelser, herunder profilering. Men, dette

lovforslag skaber hjemmel for netop profilering, hvorfor det bliver uklart præcist hvor grænsen for går det ”fuldautomatiserede” og den beslutningsunderstøttede, herunder profilering, afgørelse? I forlængelse heraf bliver det beskrevet, at man fx som sagsbehandler skal tage reelt stillingtagen til at AI-generet forslag, fx at man som sagsbehandler ikke må anvende en AI-foreslået afgørelse ”uden reelt at forholde sig til den” (s. 65). Dette er uklart, og det ville være mere korrekt at betegne denne stillingtagen som at en sagsbehandler udøver sit professionelle/forvaltningsretlige skøn.

5) Antagelser om potentialerne ved AI i lovforslaget (også påpeget i tidligere høringssvar)
    a. Lovforslaget beskriver flere steder formålet med at give hjemmel til anvendelse af AI i det offentlige. Specifikt for at understøtte kvaliteten og effektivisere i den offentlige sagsbehandling. Men hvis beslutningsstøtte implementeres fx for at sagsbehandlere skal genoverveje deres faglige vurdering, eller et AI-forslag skal fungere som et supplement til faglige vurderinger, proces og afgørelser, så kan det i praksis reelt gøre sagsbehandlingen mindre (tids)effektiv, da sagsbehandling, fordi en sagsbehandler skal forholde sig til endnu et input, tager længere tid. Derfor er det vigtigt at gøre opmærksom på, at det i praksis kan være områder, hvor det at højne kvaliteten ikke nødvendigvis gør sagsbehandling hurtigere.

Vi ser frem til at fortsætte dialogen om digitaliseringen i det offentlige, og særligt hvordan AI kan skabe værdi for borgere, ansatte, samfund og skabe et stærkt marked af leverandører, der kan bidrage med løsninger på dette område.

Med venlig hilsen

Asbjørn William Ammitzbøll Flügge
Chefkonsulent
IT-Branchen

Charlotte Holm Billund
Chefkonsulent
IT-Branchen

IT-Politisk Forening

Web: www.itpol.dk
Email: bestyrelsen@itpol.dk

11. oktober 2026

Høringssvar vedr. lovforslag om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

IT-Politisk Forening vil anbefale, at dette lovforslag **ikke fremsættes** i Folketinget. Lovforslaget søger at skabe en hjemmel til enhver brug af personoplysninger, herunder følsomme personoplysninger, til udvikling og anvendelse af AI-systemer i den offentlige sektor. Store dele af GDPR bliver reelt sat ud af kraft, herunder centrale krav som nødvendighed, proportionalitet, dataminimering og formålsbegrænsning.

Motivationen for lovforslaget synes at være, at Datatilsynet i visse situationer, hvor udvikling og anvendelse af AI-systemer indebærer indgribende behandlingsaktiviteter, har vurderet, at den eksisterende sektorlovgivning ikke udgør et tilstrækkeligt klart og præcist retsgrundlag for behandlingen af personoplysninger. Forsknings-, Uddannelses- og Digitaliseringsministeriet søger at adressere den manglende klarhed og præcision for behandling af personoplysninger til AI-systemer i det eksisterende lovgrundlag med et lovforslag, der har en endnu bredere formulering og mere generel anvendelse end den eksisterende sektorlovgivning. Det er mildest talt en besynderlig løsning på et juridisk problem, som fuldstændigt ignorerer grunden til, at der i de pågældende situationer skal være et klart og præcist retsgrundlag.

Sagt lidt firkantet kan lovforslaget opsummeres med ”alt er lovligt”, når allerede indsamlede personoplysninger behandles til udvikling og anvendelse af AI-systemer for offentlige myndigheder på grundlag af artikel 6, stk. 1, litra e i GDPR (udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse).

Efter IT-Politisk Forenings vurdering, jf. uddybningen nedenfor, er denne fremgangsmåde ikke forenelig med GDPR og Charter om Grundlæggende Rettigheder.

I den forbindelse vil IT-Politisk Forening fremhæve, at EU-retten efter EU-Domstolens retspraksis forpligter alle retsanvendende myndigheder til ikke at anvende nationale retsbestemmelser i det omfang de strider mod EU-retten. Denne pligt omfatter ikke bare danske domstole, men også Datatilsynet og andre administrative myndigheder, herunder de myndigheder som skal gøre brug af AI-hjemmelsloven. Hvis Datatilsynet vurderer, at den meget brede hjemmelsbestemmelse i lovforslagets § 3 strider mod EU-retten, vil Datatilsynet uanset den nye AI-hjemmelslov fortsat kunne træffe afgørelser om, at den eksisterende sektorlovgivning ikke udgør et tilstrækkeligt klart og præcist retsgrundlag for behandlingen af personoplysninger i forbindelse med visse AI-systemer.

Etablering af et generelt lovgrundlag for behandling af personoplysninger i AI-systemer

Lovforslagets § 3, stk. 1 søger at skabe en generel hjemmel for behandling af personoplysninger til udvikling og anvendelse af AI-systemer i den offentlige sektor.

Ifølge de specielle bemærkninger til § 3 vil et klart og tydeligt formuleret supplerende retsgrundlag, som beskriver anvendelsen af et AI-system, være nødvendigt for, at offentlige myndigheder og organer lovligt kan behandle personoplysninger ved brug af AI-systemer (i det omfang at behandlingen af personoplysninger vil være indgribende over for de registrerede). Denne formulering synes af afspejle Datatilsynets eksisterende praksis for hvorvidt den eksisterende sektorlovgivning kan udgøre et tilstrækkeligt retsgrundlag for behandling af personoplysninger ved udvikling og anvendelse af AI-systemer.

Det anføres umiddelbart derefter i bemærkningerne, at den foreslåede §3 vil medføre, at offentlige myndigheder vil have et supplerende national retsgrundlag til behandling af personoplysninger ved udvikling og anvendelse af AI-systemer (i de situationer hvor dette er nødvendigt). Konsekvensen vil være, at den enkelte myndighed ikke længere skal foretage en selvstændig vurdering af, om den eksisterende relevante sektorlovgivning har den fornødne klarhed til at udgøre et supplerende retsgrundlag efter GDPR artikel 6, stk. 3. **Den foreslåede § 3 omfatter sågar en generel hjemmel til profilering af de registrerede**, hvilket er en særdeles indgribende behandling af personoplysninger. Betragtning 71 i GDPR anfører, at profilering ikke bør omfatte en barn.

Præmissen i lovforslaget synes at være, at fordi det magiske ord ”AI” indgår direkte i § 3, stk. 1, er der nu den fornødne klarhed til enhver behandling af personoplysninger til udvikling og anvendelse af AI-systemer. Efter IT-Politisk Forenings vurdering er denne fremgangsmåde ikke forenelig med GDPR og Charter om Grundlæggende Rettigheder.

Ifølge EU-Domstolens retspraksis udgør enhver behandling af personoplysninger i den offentlige sektor et indgreb i den grundlæggende ret til databeskyttelse (artikel 8 i Charter om Grundlæggende Rettigheder). Artikel 52, stk. 1 i Charteret kræver, at indgreb i grundlæggende rettigheder skal være fastsat ved lov, respektere det væsentligste indhold af grundlæggende rettigheder, og overholde krav om nødvendighed og proportionalitet.

Den lovgivning, som indebærer en foranstaltning, der tillader et sådant indgreb, skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller mindstekrav, således at de personer, hvis personoplysninger er blevet overført, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan ske behandling af personoplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige, jf. eksempelvis EU-Domstolens dom C-175/20 præmis 55 og 83.

En lovbestemmelse, der som den foreslåede § 3, stk. 1, giver en hjemmel til enhver behandling af indsamlede personoplysninger til udvikling og anvendelse af AI-systemer, kan umuligt opfylde disse krav.

Kravet om ”fastsat ved lov” handler ikke kun om klarhed (eksempelvis at AI er omtalt på en ”klar” måde i lovbestemmelsen), men også om at retsgrundlaget skal have den fornødne præcision, således at de berørte personer kan forudsige konsekvenserne af indgrebet i deres grundlæggende rettigheder. En lovgivning, der i én sætning nærmest tillader enhver behandling af personoplysninger uden nogen reel afgrænsning, kan ikke med nogen rimelighed opfylde kravet om præcision, og overholder således ikke de basale krav til at være fastsat ved lov.

Kravet om nødvendighed kan kun være opfyldt, hvis der ikke eksisterer en mindre indgribende foranstaltning, som tillader forfølgelse af det samme legitime mål. Behandling af personoplysninger i AI-systemer vil i mange situationer indebære særdeles alvorlige indgreb i retten til beskyttelse af personoplysninger. Det skyldes bl.a. den omfattende mængde af personoplysninger, som indgår i AI-systemer, muligheden for indgribende profilering, disse modellers manglende gennemskuelighed, og ikke mindst risikoen for diskrimination eller forstærkning af eksisterende biases i den offentlige forvaltning.

På den baggrund kan kravet om nødvendighed umuligt være opfyldt for enhver behandling af personoplysninger til AI-systemer, idet der i en række tilfælde vil eksistere mindre indgribende foranstaltninger end AI-systemer.

Under alle omstændigheder er der behov for **en konkret vurdering af kravet om nødvendighed**, men formålet med den foreslåede § 3, stk. 1 er netop, at offentlige myndigheder skal kunne udvikle og anvende AI-systemer uden sådanne konkrete vurderinger af først nødvendighed og efterfølgende proportionalitet.

En vurdering af lovforslagets § 3, stk. 1 i forhold til kravene i GDPR leder til de samme konklusioner. Når det retlige grundlag for behandlingen er GDPR artikel 6, stk. 1, litra e, skal grundlaget for behandlingen fremgå af medlemsstaternes nationale ret, jf. artikel 6, stk. 3. Betragtning 41 forudsætter, at dette retsgrundlag skal være klart og præcist, og anvendelse heraf skal være forudsigelig for personer, der er omfattet af dets anvendelsesområde, jf. retspraksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol.

GDPR artikel 6, stk. 1, litra e kræver endvidere, at behandlingen skal være nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse. Betragtning 39 anfører, at personoplysninger kun bør behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde.

Disse begrænsninger i adgangen til at behandle personoplysninger (nødvendighed) er særligt relevante i forhold til AI-systemer, som generelt indebærer en omfattende og ofte særdeles indgribende behandling af personoplysninger, **og hvor der altid vil være behov for at overveje, om en mindre indgribende foranstaltning kan anvendes i stedet for AI-systemer.**

Med hensyn til kravet om nødvendighed anfører Forsknings-, Uddannelses- og Digitaliseringsministeriet i de almindelige bemærkninger pkt. 2.2.1.1, at offentlige myndigheder alene bør behandle de personoplysninger, der er nødvendige, tilstrækkelige og relevante for at kunne udvikle AI-systemet til at kunne udføre den tiltænkte opgave. Hvis behandlingsgrundlaget er artikel 6, stk. 1, litra e i GDPR gælder kravet om nødvendighed imidlertid i forhold til ”udførelse af

en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse". Et AI-system kan ikke i sig selv være en opgave i samfundets interesse.

Dertil kommer, at GDPR i artikel 5 har konkrete krav om bl.a. formålsbegrænsning og dataminimering, som enhver behandling af personoplysninger skal overholde. **Alle disse bestemmelser i GDPR bliver imidlertid fuldstændig tilsidesat af lovforslagets § 3, stk. 1**, som søger at skabe en generel hjemmel til behandling af personoplysninger i AI-systemer uden en konkret vurdering af, om denne behandling overholder GDPR (eller Charteret).

Anvendelse af personoplysninger til nye formål

Af de specielle bemærkninger til § 3 (side 70-71) fremgår det, at offentlige myndigheder kan behandle personoplysninger, som myndigheden har indsamlet til ét formål, f.eks. konkret sagsbehandling, til et andet formål, navnlig udvikling af et AI-system, **uden at skulle foretage en nærmere vurdering af, om der er tale om forenelige formål.** Det begrundes af Forsknings-, Uddannelses- og Digitaliseringsministeriet med, at der i henhold til GDPR artikel 6, stk. 4, vil være tale om viderebehandling på baggrund af national ret.

GDPR tillader imidlertid ikke enhver viderebehandling til et nyt formål uden en nærmere vurdering, da det fuldstændigt ville ophæve kravet i GDPR artikel 5, stk. 1, litra b om, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål. Denne formålsbegrænsning fremgår desuden direkte af artikel 8, stk. 2 i Charter om Grundlæggende Rettigheder. Kravet om formålsbegrænsning gælder selvsagt også for offentlige myndigheder.

Når GDPR artikel 6, stk. 4 omtaler viderehandling til et nyt formål på baggrund af national ret, er det forudsat, at denne lovbestemmelse i national ret udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1. **Denne formulering i GDPR artikel 6, stk. 4 understreger, at viderebehandling af personoplysninger til et nyt formål udgør et indgreb i den grundlæggende ret til databeskyttelse, og at dette indgreb skal opfylde krav om bl.a. nødvendighed og proportionalitet** (GDPR artikel 23, stk. 1 udmønter i den henseende kravene i Charterets artikel 52, stk. 1 for et indgreb i retten til databeskyttelse).

Lovforslaget kan således ikke, via bemærkningerne til § 3, tillade enhver viderebehandling til et nyt formål uden en konkret vurdering af, om formålene er forenelige.

Følsomme personoplysninger (GDPR artikel 9)

GDPR artikel 9, stk. 1 forbyder behandling af følsomme personoplysninger, medmindre den dataansvarlige kan påberåbe sig en af undtagelserne i artikel 9, stk. 2. Det er langt fra givet, at der i alle situationer, hvor følsomme personoplysninger behandles eller viderebehandles til et nyt formål, herunder udvikling og anvendelse af AI-systemer, kan identificeres en gyldig undtagelse i artikel 9, stk. 2. Det gælder også, hvis den dataansvarlige er en offentlig myndighed.

Lovforslagets § 3, stk. 2 synes imidlertid at være baseret på den præmis, at følsomme personoplysninger altid kan behandles til udvikling og anvendelse af AI-systemer, idet bestemmelsen alene kræver, at vedkommende minister på eget ressort skal fastsætte specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og interesser i forbindelse med behandling af følsomme personoplysninger, hvis sådanne foranstaltninger er påkrævet i henhold til databeskyttelsesreglerne.

Den underliggende antagelse synes at være, at undtagelsen i GDPR artikel 9, stk. 2, litra g generelt kan anvendes i forhold til behandling af følsomme personoplysninger i AI-systemer. Kravet i litra g er imidlertid, at behandlingen skal være nødvendig af hensyn til væsentlige samfundsinteresser, hvilket er et langt strengere nødvendighedskrav end GDPR artikel 6, stk. 1, litra e (nødvendig for udførelse af en opgave i samfundets interesse).

Det kan således ikke med nogen rimelighed antages, at enhver behandling af følsomme personoplysninger til udvikling og anvendelse af AI-systemer er nødvendig af hensyn til væsentlige samfundsinteresser.

Forsknings-, Uddannelses- og Digitaliseringsministeriet henviser i de almindelige bemærkninger pkt. 3 (side 44) til, at der generelt kan være en række potentialer forbundet med anvendelsen af AI-systemer i sagsbehandlingen, både i forhold til de anvendte ressourcer og i løftet af kvaliteten i disse opgaver. Ministeriet anfører derefter, at behandlingen af personoplysninger i forbindelse med AI-systemer derfor kan anses for at ske af hensyn til væsentlige samfundsinteresser. **Der er nærmest tale om, at Forsknings-, Uddannelses- og Digitaliseringsministeriet ophøjer anvendelsen af AI-systemer til at være en væsentlig samfundsinteresse i sig selv.**

Denne begrundelse er for det første baseret på en udokumenteret påstand om, at AI-systemer generelt fører til en mere effektiv anvendelse af ressourcer eller forbedret kvalitet af sagsbehandlingen. For det andet kan økonomiske argumenter om eksempelvis besparelser ikke i sig selv opfylde kravet om nødvendighed, og slet ikke nødvendighed af hensyn til væsentlige samfundsinteresser, hvis der er mulighed for at opfylde formålet med en mindre indgribende foranstaltning end AI-systemer (i dette tilfælde endda baseret på følsomme personoplysninger), uagtet at dette alternativ måske er mere udgiftskrævende for den offentlige myndighed.

Justitias høringssvar til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Justitia takker for modtagelsen af Digitaliseringsstyrelsens mail af 12. september 2026 om høring over forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven). I forlængelse af Justitias høringssvar af 2. marts 2026 til det tidligere lovforslag om udvikling og anvendelse af AI-systemer i den offentlige forvaltning, der bortfaldt ved udskrivelsen af folketingsvalg, fremsættes nedenstående bemærkninger til det nye lovforslag.

Justitias bemærkninger:

Generel hjemmel til udvikling og anvendelse af AI-systemer

Det foreslås i lovforslagets § 3 at indføre en generel hjemmel til, at alle offentlige myndigheder og organer, i det omfang disse behandler personoplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, og for at understøtte deres opgavevaretagelse efter anden lovgivning, kan træffe beslutning om behandling af personoplysninger til udvikling og anvendelse af AI-systemer, der kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som bl.a. kan anvendes til beslutningsstøtte, herunder evaluering af bestemte personlige forhold vedrørende en borger (profilering).

Der er efter Justitias opfattelse tale om en meget vidtgående bemyndigelse, hvorefter de enkelte ressortministre bl.a. selv kan beslutte, til hvilke formål AI-systemerne skal udvikles og anvendes, hvilke typer personoplysninger der kan behandles, samt hvilke foranstaltninger og behandlingsbetingelser, der skal iagttages, herunder hvilke krav der skal stilles til menneskeligt tilsyn og kontrol. Samtidig åbnes der op for en øget og hurtig vækst i udviklingen og anvendelsen af AI-systemer til brug for beslutningsstøtte, herunder profilering mv. i den offentlige forvaltning, hvor den hastige teknologiske udvikling løbende vil give mulighed for nye anvendelser af teknologien.

Bemyndigelsen i lovforslagets § 3 er efter Justitias opfattelse så bredt formuleret, at den ikke kan anses for at leve op til det databeskyttelsesretlige krav om klarhed, tydelighed og forudsigelighed for supplerende retsgrundlag. Derved risikerer lovforslaget at blive anset for et ugyldigt behandlingsgrundlag ved indgribende databehandling som udvikling og anvendelse af AI-systemer til beslutningsstøtte ofte kan være. Jo mere indgribende, en behandlingsaktivitet er, jo strengere er kravet til klarhed, tydelighed og forudsigelighed. Lovforslagets bemærkninger nævner også, at det vil være hjemmel til udvikling og anvendelse af ikke-indgribende AI-systemer (f.eks. tale-til-tekst, referatskrivning m.v.). til disse oplistede, specificerede og ikke-indgribende behandlingsaktiviteter, vil bemyndigelsen derimod kunne anvendes som supplerende retsgrundlag, da lovforslaget i disse tilfælde kan opfylde kravet om klar og tydelig formulering, og virkningen af lovforslaget er rimeligt forudsigeligt.

Det må efter Justitias vurdering anses for meget betænkeligt, at myndighedernes udvikling og anvendelse af AI-systemer til brug for beslutningsstøtte, herunder profilering, mv., fremover vil ske uden den sædvanlige parlamentariske kontrol og offentlige debat.

Hertil kommer, at de afledte principielle udfordringer i forhold til især borgernes rettigheder og retssikkerhed efter Justitias opfattelse ikke i tilstrækkelig grad er adresseret i lovforslaget. Justitia finder det også meget betænkeligt, at fastsættelsen af yderligere foranstaltninger for at sikre den registreredes rettigheder er formuleret som en mulighed i lovforslagets § 3 frem for et krav til de enkelte ressortministre.

Denne kritik skærpes af, at anvendelsesområdet i det reviderede lovforslag er blevet udvidet således, at også private aktører, i det omfang de udfører databehandling på vegne af det offentlige, er omfattet. Hertil kommer, at det i lovforslagets bemærkninger er anført, at anvendelsesområdet skal fortolkes bredt.

Det brede anvendelsesområde må efter Justitias opfattelse ligeledes anses for meget betænkeligt.

Undtagelser og begrænsninger af de registreredes rettigheder

I lovforslagets § 4 foreslås det at give ressortministrene samt Domstolsstyrelsen bemyndigelse til at gøre undtagelse eller begrænse de registreredes rettigheder helt eller delvist efter databeskyttelsesforordningens artikel 12 og artikel 15-21, når betingelserne for undtagelse efter databeskyttelsesforordningens artikel 23, stk. 1, er opfyldt, herunder at begrænsningen respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn en række nærmere angivne tilfælde.

Der indføres herved en vid adgang for ministrene og Domstolsstyrelsen til - hvis betingelserne i databeskyttelsesforordningens artikel 23, stk. 1, er opfyldt - at undtage og begrænse den registreredes ret til indsigt i sine data, ret til berigtigelse af sine data, ret til sletning af sine data, ret til begrænset behandling af sine data, ret til dataportabilitet og ret til indsigelse mod nærmere bestemte databehandlinger. Herudover kan ministrene undtage og begrænse den dataansvarliges forpligtelser i forhold til gennemsigtighed, oplysning og meddelelser overfor over de registrerede samt underretninger til modtagere af data. Undtagelser og begrænsninger i de registreredes rettigheder vil både kunne ske generelt på ministrenes ressortområder og konkret i forhold til et eller flere specifikke AI-systemer.

I lovforslagets bemærkninger henvises der til, at bestemmelsen vil effektivisere udviklingen af AI-systemer, som efter deres natur kan medføre en begrænsning af den registreredes rettigheder grundet AI-systemers komplekse opbygning. Det skyldes, at et AI-system i mange tilfælde er opbygget ved komplekse datastrukturer, hvor oplysninger fra mange registrerede indgår i træningsdatasæt, som ikke altid tillader adskillelse af den registreredes oplysninger, hvorfor visse af den registreredes rettigheder i praksis vil være vanskelige at overholde. Det forudsættes dog, at undtagelser og begrænsninger udelukkende fastsættes på områder, hvor det er vurderet relevant, og hvor hensynet til den konkrete behandling opvejer hensynet til at beskytte den registreredes rettigheder.

Den foreslåede bestemmelse omfatter ikke muligheden for at gøre undtagelse til den dataansvarliges oplysningspligt efter databeskyttelsesforordningens artikel 13 og 14. Det følger imidlertid af lovforslaget s. 79, at det i konkrete projekter alligevel vil være relevant at gøre undtagelse til oplysningspligten. Dette begrundes med, at databeskyttelseslovens § 22, stk. 2, vurderes at indeholde en tilstrækkelig undtagelsesmulighed, idet denne bestemmelse allerede giver mulighed for at undlade at opfylde oplysningspligten i en række nærmere definerede tilfælde. Derudover vil myndighederne i den offentlige forvaltning også i henhold til databeskyttelsesforordningens artikel 13, stk. 4, og artikel 14, stk. 5, konkret kunne vurdere, om der i specifikke situationer kan gøres undtagelse til oplysningspligten. Dette vil f.eks. være relevant i tilfælde, hvor den registrerede allerede er bekendt med oplysningerne, der fremgår af artikel 13, stk. 1-2, og artikel 14, stk. 1-2, samt i tilfælde, hvor det er umuligt at informere den registrerede om viderebehandlingen, eller i tilfælde, hvor det kræver en uforholdsmæssig stor indsats at oplyse den registrerede. De almindelige regler vedrørende aktindsigt, efter f.eks. forvaltningsloven og offentlighedsloven, vil fortsat finde anvendelse. Derfor vil myndighederne skulle sikre sig, at disse forpligtelser fortsat vil kunne overholdes.

Efter Justitias opfattelse indeholder den foreslåede bestemmelse en meget vid adgang til at begrænse de registreredes rettigheder helt eller delvist. Hertil kommer, at selvom bestemmelsen ikke giver mulighed for at gøre undtagelse til den dataansvarliges oplysningspligt efter databeskyttelsesforordningens artikel 13 og 14, gives der i lovforslagets bemærkninger alligevel mulighed for at foretage sådanne undtagelser og begrænsninger efter en konkret vurdering. Herved åbnes der op for at fravige centrale regler til beskyttelse af den registreredes rettigheder, hvilket efter Justitias vurdering må anses for meget betænkeligt. Dette sker samtidig på en særdeles ugennemsigtig måde ved "lovgivning i lovforslagets bemærkninger".

Denne kritik skærpes af det nye lovforslags bemærkninger om viderebehandling af personoplysninger. Ifølge lovforslaget vil personoplysninger, der fremgår af historiske og lukkede sager, med fordel kunne anvendes til at udvide mængden af data, der kan anvendes i AI-systemers træningsdata med henblik på at forbedre og præcisere AI-systemers output. Det gælder adgang til at anvende personoplysninger fra historiske og lukkede sager, som myndighederne og organerne på tidspunktet for udviklingen lovligt opbevarer, herunder oplysninger der ikke er overleveret til et offentligt arkiv. Viderebehandling af personoplysninger fra historiske og lukkede sager udgør en indskrænkning af en lang række af den registreredes rettigheder, herunder f.eks. retten til berigtigelse. Derved opstår en risiko for at historisk, urigtige oplysninger repliceres i AI-systemer til beslutningsstøtte, og derved tillægges vægt ved fremtidig afgørelsesvirksomhed. Dertil risikerer udvikling og anvendelse af AI-systemer at anvende historiske oplysninger på en måde, der ikke har været forudsigeligt for den registrerede, hvilket i sig selv strider med grundlæggende databeskyttelsesretlige principper. Justitia finder det meget betænkeligt, at lovforslaget hjemler viderebehandling af personoplysninger, som indsamles fra historiske og lukkede sager, til udvikling og anvendelse af AI-systemer.

I lovforslagets bemærkninger nævnes kravene i databeskyttelsesforordningen om gennemførelse af passende tekniske og organisatoriske foranstaltninger efter artikel 24, 25 og 32 samt reglerne om en

databeskyttelsesretlig konsekvensanalyse. Efter Justitias opfattelse ændrer dette dog ikke ved, at lovforslaget ikke selv opstiller konkrete materielle garantier for de registrerede. Lovforslaget overlader i vidt omfang spørgsmålet om yderligere beskyttelsesforanstaltninger til ressortministrene og Domstolsstyrelsen gennem efterfølgende bekendtgørelser uden fastsættelse af minimumskrav til sådanne garantier i loven.

Forvaltningsretlige regler og principper

Det fremgår af lovforslaget (bl.a. side 29), at det ikke vil indebære fravigelser af almindelige forvaltningsretlige regler eller principper, herunder i forvaltnings- og offentlighedsloven. Sagsbehandlingen vil derfor fortsat skulle overholde alle forvaltningsretlige regler og principper, herunder bl.a. kravet om hjemmel og saglighed, forvaltningslovens sagsbehandlingsregler samt proportionalitetsprincippet og lighedsgrundsætningen.

Modsætningsvist følger det af lovforslaget pkt. 4 om ligestillingsmæssige konsekvenser og lovforslaget s. 46-47, at der er risiko for, at borgere udsættes for forskelsbehandling på grund af muligheden for underliggende bias i AI-systemet. Bias kan ifølge lovforslaget f.eks. være en iboende del af de underliggende datasæt, navnlig når der anvendes historiske data, eller kan genereres, når systemerne implementeres under virkelige forhold. De resultater, der leveres af AI-systemer, kan påvirkes af sådanne iboende bias, som er tilbøjelige til gradvist at øges og derved videreføre og forstærke eksisterende forskelsbehandling, navnlig for personer, der tilhører bestemte sårbare grupper, herunder racemæssige eller etniske grupper. Det fremgår endvidere, at der ved at give myndigheder i den offentlige forvaltning en bred adgang til at anvende AI-systemer til at understøtte varetagelsen af deres forvaltningsopgaver efter anden lovgivning, vil være risiko for, at borgere udsættes for forskelsbehandling på baggrund af de iboende bias i AI-systemerne. Myndighederne skal derfor bl.a. selv konkret vurdere med afsæt i de relevante regelsæt, hvilke mitigerende foranstaltninger, som vil være relevante at implementere for at begrænse eventuel påvirkning fra bias i AI-systemet i forbindelse med beslutningsstøtte, herunder til evaluering af bestemte personlige forhold vedrørende en borger.

Justitia finder det meget betænkeligt, at selvom det fremgår af lovforslagets bemærkninger, at lovforslaget ikke vil indebære nogen fravigelser af alle almindelige forvaltningsretlige regler og principper i bl.a. forvaltnings- og offentlighedsloven, accepteres det andre steder i bemærkningerne, at myndighederne ikke efterlever principper om ligebehandling og ikke-diskrimination, som følger af dansk ligebehandlingslovgivning og menneskerettighedskonventionen, og at myndighederne i så fald selv skal vurdere, hvordan forskelsbehandling kan begrænses.

Justitia finder det også meget betænkeligt, at der ikke i lovforslaget er redegjort for, hvordan myndighederne ved behandling af personoplysninger til udvikling og anvendelse af AI-systemerne skal kunne overholde øvrige forvaltningsretlige regler og principper som forudsat i lovforslaget. Det gælder f.eks. retten til aktindsigt, myndighedernes notatpligt, partsindsigt mv.

Lovforslaget indeholder en væsentlig procesrisiko

Det reviderede lovforslag har indsat ordet 'profilering' i sammenhæng med de beslutningsstøttesystemer, som lovforslaget skal give mulighed for at udvikle og anvende. Kernen af

lovens formål formuleres således flere gange at være "at give offentlige myndigheder og organer adgang til at bruge AI-systemer til f.eks. beslutningsstøtte, herunder ved evaluering af bestemte personlige forhold vedrørende en borger (profilering). Begrebet skal ifølge lovforslaget forstås som det defineres i databeskyttelsesforordningens artikel 4, nr. 4.

Profilering kan indebære, at der udledes særlige kategorier af oplysninger om borgeren (såsom helbredsoplysninger, politisk eller religiøs overbevisning, race eller etnisk oprindelse, seksuelle forhold eller seksuel orientering m.v.) fra oplysninger, der ikke i sig selv udgør særlige kategorier af personoplysninger, men som bliver det, når de kombineres med andre oplysninger. Behandling af særlige kategorier af personoplysninger forbindes med særlig høj risiko, hvorfor der stilles tilsvarende højere krav til klarheden, tydelighed og forudsigeligheden af det supplerende retsgrundlag. Med anvendelsen af profilering følger desuden en række skærpede krav om at informere den registrerede om profileringen og konsekvensen heraf.

Justitia finder det meget betænkeligt at anvende så bred og uklart afgrænset lovhjemmel som behandlingsgrundlag for profilering, der i sin natur er forbundet med høj risiko for den enkelte, og derved kræver stor klarhed i behandlingens supplerende retsgrundlag.

I Databeskyttelsesforordningen har begrebet profilering størst betydning i sammenhæng med forbuddet mod at foretage automatiske individuelle afgørelser, herunder profilering.

Hvad angår profilering, fremgår det af lovforslaget, at det skal udgøre hjemmel til beslutningsstøttesystemer, men ikke fuldautomatiske individuelle afgørelser, herunder profilering efter artikel 22, stk. 1.

Af lovforslaget fremgår følgende:

> "Kravet om hvor stor den menneskelige involvering skal være, førend der er tale om beslutningsstøtte og ikke fuldautomatiske afgørelser eller tiltag, er ikke fastlagt klart i praksis. Det må derfor forventes, at fremtidig praksis vil bidrage til at præcisere, hvilken grad af menneskelig involvering der kræves for, at anvendelsen af et AI-system kan anses som beslutningsstøtte efter den foreslåede ordning og ikke fuldautomatiske afgørelser eller tiltag, f.eks. efter databeskyttelsesforordningens artikel 22 om automatiske individuelle afgørelser, herunder profilering."

Justitia finder det meget betænkeligt, at man ved lovforslagets vedtagelse accepterer en væsentlig procesrisiko.

En af de mest alment kendte risici ved at anvende AI beslutningsstøtte, er det såkaldte 'Automation Bias', hvor et AI-systems forslag til afgørelse tillægges uforholdsmæssigt stor vægt af den enkelte sagsbehandler, og over tid tillægges så meget vægt, at systemet de facto afgør sagen, og at afgørelsen således kan sidestilles med en fuldautomatisk individuel afgørelse efter databeskyttelsesforordningens artikel 22.

Artikel 29-gruppen har udtalt i sine retningslinjer om automatiske individuelle afgørelser og profilering, at det, for at der kan være tale om menneskelig kontrol, skal sikres, at tilsyn med afgørelsen er meningsfuldt og ikke blot en formalitet.

Justitia finder det meget betænkeligt, at lovforslaget ikke indeholder vidtrækkende garantiordninger, der sikrer et højt og vedvarende beskyttelsesniveau tilsvarende de høje beskyttelseskrav, der følger af undtagelsesbestemmelsen til forbuddet mod fuldautomatiske individuelle afgørelser, herunder profilering i databeskyttelsesforordningens artikel 22, stk. 2.

Justitias anbefalinger:

Myndighedernes behandling af personoplysninger til udvikling og anvendelse af AI-systemer skal fortsat ske direkte ved lov, og lovforslagene skal indeholde fyldestgørende redegørelser for de foreslåede AI-systemers udvikling og påtænkte anvendelse.

Myndighedernes behandling af personoplysninger til udvikling og anvendelse af AI-systemer til brug for beslutningsstøtte, profilering mv. indebærer store ændringer af vores samfund og væsentlige påvirkninger af borgerens rettigheder og retssikkerhed. Det er Justitias vurdering, at en sådan samfundsudvikling og den konkrete regulering af udvikling og anvendelse af de enkelte AI-systemer bør være underlagt løbende parlamentarisk kontrol. Det er på denne baggrund Justitias anbefaling, at reguleringen af myndighedernes behandling af personoplysninger til udvikling og anvendelse af AI-systemer fortsat skal ske ved direkte ved lov fremfor vidtgående bemyndigelser til ressortministrene og Domstolsstyrelsen.

Som det fremgår af Justitias rapport *Udfordringer i lovgivningsprocessen* fra juli 2024, bliver de problemstillinger, der generelt karakteriserer lovgivningsprocessen, forstærket, når lovforslag indeholder digitalisering og anvendelse af ny teknologi.

Justitia anbefaler derfor, at der også stilles krav om, at lovforslaget skal indeholde fyldestgørende redegørelser for de foreslåede AI-systemers udvikling og påtænkte anvendelse, herunder resultatet af de forskellige konsekvensanalyser og lignende, der skal foretages efter de forvaltningsretlige, databeskyttelsesretlige og AI-retlige rammer, med særlig fokus på risici i forhold til borgernes rettigheder og retssikkerhed.

Hvis lovforslaget alligevel vedtages, bør det kun omfatte ikke-indgribende behandlinger

Som tidligere anført vurderer Justitia, at lovforslaget ikke lever op til det databeskyttelsesretlige krav om et klart og tydeligt supplerende retsgrundlag, hvor anvendelsesområdet er forudsigeligt for den registrerede. Hvis lovforslaget alligevel vedtages, bør det indskrænkes til kun at omfatte en udtømmende liste af udspecificerede, ikke-indgribende behandlinger af personoplysninger.

Hvis lovforslaget alligevel vedtages, bør Justitsministeriet være resortmyndighed

Hvis lovforslaget alligevel vedtages, vil Justitia desuden anbefale, at bemyndigelse til at gøre undtagelse eller begrænse de registreredes rettigheder efter databeskyttelsesforordningen eller almindelige forvaltningsretlige regler og principper i bl.a. forvaltnings- og offentlighedsloven, skal udøves med stor forsigtighed og gives til Justitsministeriet som resortmyndighed for disse regelsæt fremfor ministrene på de områder, hvor systemernes skal udvikles og anvendes.

Hvis lovforslaget alligevel vedtages, skal Folketinget årligt orienteres om udvikling og anvendelse af nye AI-systemer.

Justitia vil endvidere anbefale, at regeringen en gang årligt skal orientere Folketinget om udvikling og anvendelse af nye AI-systemer, der kan generere output som forudsigelser, indhold, anbefalinger eller beslutninger, herunder profilering. Orienteringen skal indeholde fyldestgørende redegørelser for resultatet af de forskellige konsekvensanalyser og lignende, der skal foretages efter de forvaltningsretlige, databeskyttelsesretlige og AI-retlige rammer med særligt fokus på risici i forhold til borgernes rettigheder og retssikkerhed.

Myndighederne skal under alle omstændigheder løbende orientere Folketinget og offentligheden om, hvordan AI- systemerne virker i praksis.

Uanset, om lovforslaget vedtages, bør der efter Justitias opfattelse stilles krav om, myndighederne løbende, f.eks. årligt, skal orientere Folketinget og offentligheden om, hvordan systemerne virker i praksis, herunder om konstaterede fejl og risici, og hvilke foranstaltninger dette har givet anledning til.

Med venlig hilsen

Birgitte Arent Eiriksson
Direktør Justitia Danmark

JUSTITIA
E-mail: birgitte@justitia-int.org
http://www.justitia-int.org

Eric Thyrgaard Jensen
Jurist

JUSTITIA
E-mail: eric@justitia-int.org
http://www.justitia-int.org

NOTAT

Digitaliseringsstyrelsen

Sendt pr. mail til jon-mei@digst.dk, emimol@digst.dk, leaomd@digst.dk, og kahevi@digst.dk den 9. Oktober 2026

KL's høringssvar til lovforslag om udvikling og anvendelse af AI ved behandling af personoplysninger

Dato: 09-10-2026

Sags ID: SAG-2026-00619
Dok. ID: 3735490

E-mail: SFB@kl.dk/
LOMJ@kl.dk
Direkte: +45 3370 3909

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Digitaliseringsstyrelsen har den 12. september 2026 sendt udkast til lovforslag om Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven) og bedt om KL's bemærkninger.

KL bakker op om lovforslaget, der giver den længe efterspurgte supplerende hjemmel til, at offentlige myndigheder kan udvikle og anvende AI-systemer til behandling af alle typer af personoplysninger. KL finder det positivt, at hjemlen i lovforslagets § 3, stk. 1, udtrykkeligt omfatter muligheden for at foretage profilering til brug for bl.a. beslutningsstøtte.

Det er endvidere positivt, at lovhjemlen efter KL's opfattelse omfatter alle myndighedsopgaver i kommunerne – både myndighedsafgørelser og faktisk forvaltningsvirksomhed.

KL er imidlertid opmærksom på, at lovforslaget er svar på én blandt flere problemstillinger. Øvrige compliancekrav er fortsat uforandrede, hvilket også fremgår af bemærkningerne til lovforslaget.

Med lovforslaget signaleres der vilje til at gøre det muligt for myndigheder at udvikle og anvende AI-løsninger bredt.

KL's hovedbudskaber

- KL bakker op om lovforslagets formål, som giver kommuner og andre offentlige myndigheder det efterspurgte supplerende hjemmelsgrundlag for bred anvendelse af AI-løsninger med alle kategorier af personoplysninger på tværs af fagområder, herunder til brug for beslutningsstøtte.

- KL er enig i, at det er nødvendigt, at der indføres en bemyndigelsesbestemmelse, som kan fungere som en ventil-bestemmelse, der sikrer muligheden for, at ministre på de respektive ressortområder kan udstede bekendtgørelser, hvis der opstår behov for det.

- KL foreslår, at der udpeges en koordinerende enhed, som sikrer ensartede vurderinger på tværs af ministerområder og fungerer som ét samlet kontaktpunkt for kommuner og andre myndigheder ved spørgsmål om lovens anvendelse og behovet for eventuel supplerende

Dato: 01-10-2026

Sags ID: SAG-2026-00619
Dok. ID: 3735490

E-mail: SFB@kl.dk
Direkte: +45 3370 3909

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

regulering og vejledning, samt sikrer standardisering af eventuel supplerende regulering.

- KL bemærker, at lovforslagets beskrivelse af grænsen mellem beslutningsstøtte og fuldautomatiske afgørelser er uklar og efterlader kommunerne med en betydelig usikkerhed, når de skal udvikle og tage nye AI-systemer i brug. Der er derfor allerede ved lovens ikrafttræden behov for tydelige rammer og vejledning for brugen og grænserne for brugen af beslutningsstøtte.

- KL bakker op om muligheden for proportionale begrænsninger af de registreredes rettigheder inden for rammerne af databeskyttelsesforordningen, forudsat at borgernes rettigheder og de nødvendige retssikkerhedsgarantier samtidig sikres.

Nedenfor følger KL's bemærkninger til konkrete dele af lovforslaget.

Bemærkninger til § 2 om definitioner

Lovforslaget retter sig mod udvikling og anvendelsen af AI-systemer, som de er defineret i AI-forordningen. Det er væsentligt, at loven er smidig i forhold til den teknologiske udvikling og i forhold til forekomsten af nye digitale løsninger, som relaterer sig til AI og til eksisterende mere simple AI-systemer, for at sikre, at der også er hjemmel til at udvikle og anvende sådanne løsninger.

KL foreslår, at det sikres, at loven er teknologineutral i forhold til AI-systemer, sådan at loven i sit anvendelsesområde også favner løsninger der minder om AI-systemer. Dette fokus på lignende digitale løsninger benyttes allerede i bekendtgørelsen om kommunernes behandling af personoplysninger med kunstig intelligens i beskæftigelsesindsatsen. Her dækker begrebet "lignende digitale løsninger" over løsninger, der har karakteristika svarende til kunstig intelligens, uden at en sådan løsning falder inden for definitionen af kunstig intelligens i AI-forordningen. Begrebet "lignende digitale løsninger" sikrer dermed, at der tages højde for den teknologiske udvikling, således at nye teknologier, der minder om kunstig intelligens uden at opfylde de eksakte krav i AI-forordningen, vil være omfattet. Det anbefales derfor, at "lignende digitale løsninger" tilføjes definitionen med henblik på at sikre, at der ikke opstår asymmetri på tværs af fagområder og lovgivninger.

Definition af beslutningsstøtte
Begrebet beslutningsstøtte, der står beskrevet i lovens § 2, stk. 4, er søgt afgrænset i lovforslagets bemærkninger. Det fremgår bl.a. heraf, at begrebet allerede i dag anvendes på sundhedsområdet, og begrebet derfor skal forstås i overensstemmelse hermed. KL foreslår, at det i bemærkningerne bliver uddybet, hvordan begrebet anvendes på andre områder, som fx sundheds- og beskæftigelsesområderne for at tydeliggøre og sikre, at der ikke opstår uhensigtsmæssige og i værste fald modstridende forståelser af begrebet beslutningsstøtte.

Dato: 01-10-2026

Sags ID: SAG-2026-00619
Dok. ID: 3735490

E-mail: SFB@kl.dk
Direkte: +45 3370 3909

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Uklar grænse mellem beslutningsstøtte og fuldautomatiske afgørelser
KL finder det positivt, at hjemlen i lovforslagets § 3, stk. 1, udtrykkeligt omfatter muligheden for at foretage profilering til brug for beslutningsstøtte. Lovforslaget giver ikke mulighed for fuldautomatiserede afgørelser. KL bemærker, at det ikke kan udelukkes, at der på sigt kan være behov for denne mulighed på konkret afgrænsede områder, hvor det vurderes hensigtsmæssigt.

Ift. forskellene mellem beslutningsstøtte og fuldautomatiske afgørelser eller væsentlige tiltag fremgår det af de specielle bemærkninger til § 2, nr. 4, og til § 3, stk. 1, at det må forventes, at fremtidig praksis vil sætte denne grænse. Altså hvad der kræves af menneskelig involvering for at AI-støtte til sagsbehandling mv. kan kategoriseres som beslutningsstøtte og ikke som en fuldautomatisk afgørelse. Lovforslaget giver ikke en klar beskrivelse af denne grænse, og det kan efterlade kommunerne med en betydelig usikkerhed, når de skal udvikle og tage nye AI-systemer i brug. Udfordringen bliver bl.a., hvilke sikkerhedsforanstaltninger der er nødvendige for at undgå såkaldt "automation bias", hvis AI-systemets forslag bliver lagt ukritisk til grund, i stedet for at gennemgå en reel efterprøvelse af sagsbehandleren. Der er derfor allerede ved lovens ikrafttræden behov for tydelig vejledning om grænserne for brugen af beslutningsstøtte.

Bemærkninger til § 3 om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Hjemmel til behandling af alm. personoplysninger, følsomme oplysninger og oplysning om strafbare forhold
KL finder det positivt, at kommunerne får supplerende hjemmel til anvendelse af AI-systemer til behandling af personoplysninger. KL har forstået lovforslaget sådan, at § 3, stk. 1, giver hjemmel til behandling af både almindelige personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, særlige kategorier af personoplysninger (følsomme oplysninger) efter artikel 9, stk. 1, og oplysninger om strafbare forhold efter artikel 10. KL anmoder om, at denne forståelse kommer til at fremgå endnu tydeligere af bemærkningerne til § 3, stk. 1, så der ikke kan opstå tvivl om forståelsen. KL foreslår, at det præciseres i lovbemærkningerne, at den foreslåede hjemmel eksempelvis vil kunne anvendes til det beslutningsstøtteværktøj i Københavns Kommune, som Datatilsynet tog stilling til den 17. november 2023 (journalnummer 2023-212-0015), forudsat at kommunen overholder de øvrige gældende compliancekrav.

Det er endvidere positivt, at anvendelsesområdet siden første høringsrunde er blevet udvidet til at omfatte den fulde ordlyd af databeskyttelsesforordningens artikel 6, stk. 1, litra e, således at myndigheder og organer, der løser opgaver i samfundets interesse, også er omfattet af lovens anvendelsesområde, og ikke kun myndigheder og organer, der løser opgaver, der henhører under offentlig myndighedsudøvelse.

KL vurderer, at det bør stå klarere, hvad "efter anden lovgivning" omfatter i § 3, stk. 1, og at det sikres, at behandlinger, der foretages på grundlag af

Dato: 01-10-2026

Sags ID: SAG-2026-00619
Dok. ID: 3735490

E-mail: SFB@kl.dk
Direkte: +45 3370 3909

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

kollektive overenskomster, også dækkes af den foreslåede hjemmel. Hvis Digitaliseringsstyrelsen vurderer, at kollektive overenskomster kan rummes inden for formuleringen " efter anden lovgivning" bør kollektive overenskomster nævnes i lovbemærkningerne. Det bør også fremgå klart af lovbemærkningerne, at behandlingen på grundlag af ulovbestemte regler som fx kommunalfuldmagten, anstaltsforhold og andre almindelige ulovbestemte retsgrundsætninger er omfattet af "efter anden lovgivning".

Oplysninger, som myndighederne behandler
Det bør i de almindelige bemærkninger om gældende ret beskrives i hvilket omfang myndighederne kan udvikle AI-systemer på grundlag af offentligt tilgængelige personoplysninger, fra fx Sprogteknologi.dk. Det samme gælder med hensyn til udvikling af AI-systemer, som ikke kræver, at den dataansvarlige selv råder over de samlede datasæt, men flere dataansvarlige kan udvikle på det samme AI-system uden at dele egne datasæt (fødereret læring), som beskrevet i Datatilsynets vejledning "Offentlige myndigheders brug af kunstig intelligens – inden I går i gang", fra 2023. Som lovbemærkningerne er formuleret i høringsudkastet, beskrives det alene, hvad man ikke kan. Det kan føre til usikkerhed om, hvilke data offentlige myndigheder kan indsamle på grundlag af anden regulering eller på grundlag af andre metoder.

Nødvendig bemyndigelsesbestemmelse med risiko for uklar retstilstand
KL forstår forslagets § 3, stk. 2, sådan, at bestemmelsen ikke etablerer det supplerende behandlingsgrundlag for følsomme personoplysninger og oplysninger om strafbare forhold, som er etableret i lovens § 3, stk. 1, men er tænkt som en bemyndigelsesbestemmelse for vedkommende ressortministre til i visse tilfælde, hvis det viser sig at være behov herfor at udstede bekendtgørelse om "passende og specifikke foranstaltninger", hvor der behandles følsomme personoplysninger eller oplysninger om strafbare forhold.

KL noterer sig, at der ikke er beskrevet en generel pligt til at udstede bekendtgørelser, men at behovet skal vurderes konkret. Efter dialog med kommunerne kan KL konstatere, at der er usikkerhed om rækkevidden og forståelsen af samspillet mellem § 3, stk. 1 og 2. Det bør derfor præciseres i lovbemærkningerne, hvornår bemyndigelsesbestemmelsen er tænkt anvendt.

Hvis intentionen er, at det er en snæver "ventil"-bestemmelse, fordi passende og specifikke foranstaltninger er dækket i det compliancearbejde, der allerede finder sted ved myndighederne, og bestemmelsen derfor kun skal anvendes helt undtagelsesvist, bør det fremgå klart af bemærkningerne. Hvis bestemmelsen er tiltænkt de tilfælde, hvor der opstår behov for en tværgående bekendtgørelse, der dækker flere ressortområder, og som skal hjælpe myndigheder med at fastsætte tværgående og fælles passende og specifikke minimumsforanstaltninger til brug for et større AI-system, der kan anvendes på tværs af fx alle kommunerne, vil det også være hjælpsomt, at det fremgår tydeligt af bemærkningerne.

Dato: 01-10-2026

Sags ID: SAG-2026-00619
Dok. ID: 3735490

E-mail: SFB@kl.dk
Direkte: +45 3370 3909

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

KL foreslår, at der udpeges en koordinerende enhed, som fx Den Digitale Taskforce for Kunstig Intelligens, som skal koordinere og sikre ensartede vurderinger på tværs af relevante ministerområder og fungere som ét samlet kontaktpunkt for kommuner og andre myndigheder ved spørgsmål om lovens anvendelse og behovet for eventuel supplerende regulering.

Hvis der udstedes bekendtgørelser efter § 3, stk. 2, anbefaler KL desuden, at der så vidt muligt anvendes en ensartet model på tværs af ressortområder. Det vil understøtte en mere ensartet implementering af loven og reducere risikoen for retlig usikkerhed.

AI-loven skal suppleres af vejledningsindsats
KL finder det væsentligt, at lovforslaget følges op af en klar og praksisnær vejledning. Loven giver myndighederne den længe efterspurgte lovhjemmel, men løser ikke en lang række vanskelige spørgsmål om samspillet med bl.a. sektorlovgivningen, databeskyttelsesretten, AI-forordningen og forvaltningsretten, som myndighederne skal kunne håndtere i praksis, hvorfor det er nødvendigt, at det omsættes til klare, ensartede og operationelle krav.
Udfordringer med eksempelvis gennemsigtighed, kvalitetssikring, saglighed og ligebehandling samt effektiv menneskelig kontrol ved brug af AI er fælles anliggender, der kræver fælles løsninger. Vejledning bør derfor tydeliggøre og samtænke, hvilke krav myndighederne skal opfylde og hvordan, når AI-løsninger udvikles og tages i brug. Det vil bidrage til en ensartet fortolkning af reglerne og mindske den retlige usikkerhed. Vejledning bør derfor samtænke de mange krav, og bør foreligge samtidig med lovens ikrafttræden, så kommunerne fra start har et klart og sikkert grundlag for at anvende de nye muligheder. KL bidrager gerne til at tilrettelægge vejledningsindsatsen, herunder med konkrete kommunale cases, så vejledningen tager afsæt i de spørgsmål og udfordringer, kommunerne møder i praksis.

Bemærkninger til § 4 om undtagelse til den registreredes rettigheder
KL noterer, at lovforslagets § 4 bemyndiger ressortministrene til ved bekendtgørelse at fastsætte begrænsninger i de registreredes rettigheder efter databeskyttelsesforordningens artikel 12 og 15-21 inden for rammerne af artikel 23.

KL støtter muligheden for nødvendige og proportionale begrænsninger, når borgernes rettigheder og de nødvendige retssikkerhedsgarantier samtidig sikres. KL efterlyser, at der i bemærkninger til lovforslaget eller i en supplerende vejledning laves en tydelig beskrivelse af, i hvilke situationer på de kommunale områder bemyndigelsen kunne forventes anvendt, og hvilke hensyn der kan begrunde begrænsningerne, da det er KL's vurdering, at mulighederne uden nærmere regulering vil være meget begrænsede.

Bemyndigelsen omfatter ikke oplysningspligten efter databeskyttelsesforordningens artikel 13 og 14. Bemærkningerne henviser i stedet til, at databeskyttelseslovens § 22, stk. 2, giver tilstrækkelig mulighed for at fravige oplysningspligten i konkrete projekter. KL efterlyser konkrete eksempler på sådanne AI-projekter, herunder hvilke offentlige

hensyn der kan begrunde undtagelse, og hvordan disse skal afvejes over for borgernes interesse i at blive informeret.

KL ønsker desuden, at det skal klargøres, hvordan oplysningspligten i praksis forudsættes håndteret ved AI-systemer, der indebærer behandling af oplysninger om et stort antal registrerede, herunder under hvilke betingelser generel information, fx via kommunes hjemmeside, kan træde i stedet for individuel underretning. Dette kan med fordel tydeliggøres i bemærkningerne til lovforslaget.

KL står til rådighed for nærmere uddybning af vores bemærkninger til lovforslaget.

Med venlig hilsen

Christian Harsløf

Direktør, KL

Dato: 01-10-2026

Sags ID: SAG-2026-00619
Dok. ID: 3735490

E-mail: SFB@kl.dk
Direkte: +45 3370 3909

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

KOMBIT A/S
Halfdansgade 8
2300 København S

Tlf. +45 33 34 94 00
kombit@kombit.dk
www.kombit.dk

CVR-nr.: 19435075
EAN-nr. 5790001969370

12. oktober 2026

NOTAT

Høringssvar til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Introduktion

KOMBIT er et kommunalt ejet it-fællesskab, der er ansvarlig for at indkøbe, forvalte, drifte og videreudvikle tidssvarende og stabile it-løsninger samt -infrastruktur til landets 98 kommuner til gavn for borgere og virksomheder.

KOMBIT bidrager på den baggrund med viden og erfaringer om fælleskommunale it-løsninger og infrastruktur, også inden for AI-løsninger, til lovforslaget.

KOMBIT har følgende bemærkninger og anbefalinger til lovforslaget, at:

§ 1 og § 3, stk. 2 anvendelsesområde i forhold til databeskyttelsesforordningen fremstår uklar

Det følger af ordlyden af lovforslagets § 1, at loven vil gælde for behandling af personoplysninger, der sker med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e. Den foreslået ordlyd af lovforslagets § 1 kan forstås således, at der ikke er et selvstændigt grundlag til brug af AI ved behandling af særlige kategorier af personoplysninger efter forordningens artikel 9 og databeskyttelsesloven, herunder om personnumre i henhold til § 11.

Behovet – og udgangspunktet – for lovforslaget er, at denne har til formål at gøre det lettere for offentlige myndigheder at anvende AI, herunder generativ AI, på en ansvarlig og sikker måde på tværs af almindelige arbejdsopgaver, sagsbehandling og beslutningsstøtte. Anvendelse af AI kan bidrage til en mere effektiv opgaveløsning, og på sigt også styrke borgernes retssikkerhed i afgørelsessager, eksempelvis via mere ensartet sagsbehandling.

Ved den nuværende afgrænsning af lovforslagets § 1 til alene almindelige personoplysninger (ikke-følsomme personoplysninger) fremstår det således, at myndigheder imidlertid ikke kunne anvende AI-systemer i sager, der indeholder særlige kategorier af personoplysninger. Det gælder for en væsentlig del af kommunernes opgaver, herunder på eksempelvis social-, beskæftigelses- og sundhedsområdet, hvor sager kan indeholde en flerhed af oplysninger. Videre vil afgrænsningen i sig selv medfører en uhensigtsmæssig og kunstig opdeling af myndighedernes arbejde og begrænse brugen af AI på tværs af alle relevante oplysninger, enten følsomme eller ikke-følsomme personoplysninger

KOMBIT anbefaler, at lovforslagets § 1 anvendelsesområde udvides til også at omfatte andre kategorier af personoplysninger, herunder behandling af særlige kategorier af personoplysninger med udgangspunkt i databeskyttelsesforordningen og databeskyttelseslovens bestemmelser, og med

fastsættelse af passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

En sådan udvidelse vil gøre det muligt at regulere og tydeliggøre foranstaltninger, der skal gælde ved behandling af andre kategorier af oplysninger, så myndighederne bredt kan anvende AI ansvarligt og i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesloven og øvrig relevant lovgivning.

§ 3, stk. 1 kan specificeres

Det følger af lovforslagets § 3, stk. 1 at offentlige myndigheder og organer kan udvikle og anvende AI-systemer.

Det anbefales at det specificeres eller præciseres yderligere i bemærkningerne, at hjemlen ligeledes kan gælde for offentlige myndigheders leverandører og deres udvikling af enten individuelle og/eller fællesstatslige AI-systemer og AI-assistenter til brug for offentlige myndigheder.

KOMBIT anbefaler videre, at det præciseres under hvilke betingelser personoplysninger fra flere kommuner og/eller andre myndigheder og på tværs af retsområder kan anvendes til træning af fælles AI-systemer, eksempelvis når KOMBIT udvikler fællesoffentlige AI-assistenter og AI-løsninger til flere kommuner. En sådan afklaring kan være en forudsætning for at kunne udvikle fællesoffentlige AI-assistenter og AI-systemer, der kan give bedre og mere ensartede resultater.

§ 3, stk. 2 kan medføre uklar retstilstand

Det følger af lovforslagets § 3, stk. 2 at vedkommende minister inden for sit ressortområde kan fastsætte passende og specifikke foranstaltninger, når behandlingen omfatter personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, eller artikel 10 herunder, hvis sådanne foranstaltninger er på krævet i henhold til databeskyttelsesreglerne.

Vores primære bemærkning er, at ordlyden af denne bestemmelse skaber uklarhed i forhold til lovforslagets § 1, hvor anbefalingen fra KOMBIT er at udvide, subsidiært specificere anvendelsesområde, jf. ovenstående bemærkninger.

Videre specificeres det ikke i udkastet til loven eller i bemærkningerne, hvilke foranstaltninger, hvem de skal gælde for, hvilke AI-systemer (eksempelvis kun højrisiko AI-systemer) eller hvornår foranstaltningerne eventuelt vil træde i kræft – og ydermere specificeres det ikke, hvilken retstilstand der vil være gældende frem til at de specifikke ressortområder fastlægger andre eller øvrige foranstaltninger.

Et af lovforslagets hovedformål er at skabe klarhed om offentlige myndigheders brug af AI. Den valgte model indebærer dog en risiko for det modsatte – idet det ikke er afklaret, hvem, til hvilken brug eller hvilke AI-systemer der vil være omfattet af lovforslagets § 3, stk. 2.

Hertil bemærkes ydermere en materiel risiko for, at forskellige ministerier eller styrelser vil fastsætte forskellige krav, så der potentielt opstår parallelle retstilstande for eksempelvis højrisiko AI-systemer. Det vil være særligt udfordrende for kommunerne og for fælleskommunale løsninger, der går på tværs af flere ressort- og retsområder.

KOMBIT anbefaler, at

- det præciseres, hvilke krav der vil gælde, indtil der er fastsat ressortspecifikke foranstaltninger (forudsat at bestemmelsen fastholdes);
- det sikres, at de ressortansvarlige ministerier fastsætter ensartede og koordinerede krav, så der ikke opstår parallelle retstilstande for myndighedernes brug af AI.

Afslutning

KOMBIT takker for muligheden for at give bemærkninger til lovforslaget.

Endeligt bemærker KOMBIT, at KOMBIT ligeledes bakker op om indholdet af KL's høringssvar, herunder KL's hovedbudskaber om lovforslaget.

KOMBIT står meget gerne til rådighed for en nærmere dialog vedrørende udformningen og skriv af hjemmel til offentlige myndigheders og organers udvikling og anvendelse af AI-systemer. I er velkommen til at kontakte KOMBIT direkte via MRS@kombit.dk, att. Johanne Strabo Svendsen.

Med venlig hilsen

Johanne Strabo Svendsen

Direktør for Compliance, Kvalitet & Sikkerhed

KIT Informationssikkerhed (6957)
Økonomiforvaltningen

Høringssvar

Til Forsknings-, Uddannelses- og Digitaliseringsstyrelsen

Høringssvar til Forslag til Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

15-09-2026

Sagsnummer i F2
2026 - 20422

Dokumentnummer i F2
12057414

Sagsnummer eDoc

Sagsbehandler
Amalie Viinberg Henriksen
Nelli Schubert Jensen

Generelle bemærkninger

Københavns Kommune bemærker, at det er positivt, at Digitaliseringsstyrelsen med det kommende lovforslag ønsker at løse nogle af de mere komplekse nationale hjemmelsproblematikker for så vidt angår udvikling, test og anvendelse af AI ved behandling af personoplysninger i offentlige myndigheder. Det er vigtigt for kommunen, at de forbedrede muligheder der følger af loven, hurtigt implementeres hos relevante statslige myndigheder. Kommunen ønsker i den anledning at kvittere for det forsatte gode arbejde, som Digitaliseringsstyrelsen har lagt i det nuværende lovforslag hen over sommeren.

Resumé

Digitaliseringsstyrelsen har den 14. september 2026 sendt udkast til forslag til lov om offentlige myndigheders og organers udvikling af anvendelse AI-systemer ved behandling af personoplysninger i høring.

Det fremgår af bemærkningernes s. 15, at lovforslaget ikke skal ophæve anden gældende sektorlovgivning, som regulerer samme anvendelsesområder. Kommunen anser det som værende positivt, at Digitaliseringsstyrelsen vil sikre kontinuitet på tværs af retsområder ved at bevare hjemlerne i sektorlovgivningen, men bemærker også, at det bidrager til en kompliceret retstilling at have parallelle hjemler på tværs af lovgivninger. Kommunen anser det også for positivt, at Digitaliseringsstyrelsen opfordrer til, at der i forbindelse med fremtidig revision af sektorlovgivning overvejes, om hjemlen til behandling af personoplysninger kan findes i dette lovforslag fremfor regulering i sektorlovgivningen.

Det fremgår af s. 34, at "den foreslåede ordning vil betyde, at der vil blive etableret et grundlag for viderebehandling af

personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 4, som myndigheden allerede er i besiddelse af og har lovlig adkomst til". I forhold til udvikling af stabile og korrekte AI-systemer, ser kommunen positivt på, at kommunen kan anvende lukkede sager til at træne en AI. Kommunen vil anse det som værende positivt, hvis denne hjemmel var tydeligere i paragrafferne fremfor en del af bemærkningerne, da det vil tydeliggøre kommunens råderum.

Kommunen som offentligt myndighed kommer i klemme mellem henholdsvis Digitaliseringsstyrelsen og Datatilsynets forståelse af hjemmelsspørgsmålet for udvikling og drift af AI-systemer. Der opfordres til, at dette tvivlsspørgsmål afklares, da kommunen risikerer at have en uklar retsstilling.

§1

Det er positivt, at paragraffen specificerer, hvem der har adgang til at anvende paragraffen.

Det anses dog som værende problematisk, at loven om en kommende AI-hjemmel kun giver hjemmel til at bruge AI til behandling af personoplysninger med hjemmel i databeskyttelsesforordningen artikel 6, stk. 1 litra e. Som offentlig myndighed der er pålagt en række lovpligtige opgaver, vil behandling af almindelige personoplysninger også kunne have hjemmel i databeskyttelsesforordningen artikel 6, stk. 1, litra b og c, og kommunen vil derfor ikke kunne bruge AI til at løfte den type af opgave. Disse kan være ressourcetunge men rutinepræget, og kommunen ser derfor et potentiale, som ikke kan blive udforsket med den nuværende begrænsning af hjemmel. Et andet aspekt er, at udvikling af AI-systemer med borgerdata, oftest vil kræve, at der også vil blive behandlet medarbejderoplysninger. Denne behandling kan have hjemmel i andre artikel 6 behandlingsgrundlag, og forslaget med litra e er derfor begrænsende på en uhensigtsmæssig måde.

Det anses endvidere som problematisk, at der ikke gives generel hjemmel til behandling af personoplysninger med hjemmel i artikel 9, og at denne gøres afhængig af ressortspecifikke hjemmelsudstedelser i medfør af §3, stk. 2.

Alternativt kunne afgrænsningen tage udgangspunkt i forvaltningsloven, retsplejeloven og retssikkerhedsloven § 43, stk. 1, sådan som bemærkningernes s. 26 også beskriver.

§2, nr. 1

Det kunne være hensigtsmæssigt at indarbejde en supplering, så det ikke kun er AI-systemer, der lærer undervejs/har en varierende grad af autonomi. F.eks. på beskæftigelsesområdet har man i sektorlovgivningen valgt formuleringen "kunstig intelligens eller lignende digitale løsninger" for at fremtidssikre lovgivningen med en bredere definition.

Det fremgår af s. 61, at lovforslaget kun er en hjemmel til brug af AI-systemer i overensstemmelse med definitionen af AI-systemer i Forordningen for Kunstig Intelligens. Som tidligere anført, er inklusionen af kravet om varierende grad af autonomi afgrænsende i forhold til andre teknologier, som ikke har nogen form for autonomi, men som fortsat kræver en hjemmel. Kommunen vil derfor opfordre til, at man genovervejer og eventuelt genbruger formuleringen fra sektorlovgivningen på beskæftigelsesområdet "kunstig intelligens eller lignende digitale løsninger", da det blandt andet vil omfatte teknologi, som ikke har en varierende grad af autonomi.

§2, nr. 2

Det vil være hensigtsmæssigt i lovforslaget at anvende formuleringen, at det er "den til en hver tid gældende definition af en personoplysning jf. databeskyttelsesforordningen". På den måde er lovforslaget neutralt i relation til, hvordan resultatet af den digitale omnibus 2026 falder ud.

Kommunen ser udover ovenstående forhold positivt på, at lovforslaget anvender begreber i overensstemmelse med velkendte definitioner fra andre EU-retlige og nationale lovgivninger.

§2, nr. 3

Eftersom det er intentionen, at en offentlige myndighed skal kunne profilere, kan det være hensigtsmæssigt at anvende ordet "profilering", så det ikke efterlader et fortolkningsrum.

§2, nr. 4

Det foreliggende grundlag bør præciseres i lovforslaget, så det er klart i relation til muligheden for profilering jf. databeskyttelsesforordningens artikel 22, også selvom man ikke kan træffe automatiserede afgørelser.

§ 3, stk. 1

Anvendelsesområdet bør defineres bredere i lovforslaget, således at også mindre indgribende versioner af nyere teknologi indenfor AI kan anvendes og omfattes af lovforslaget f.eks. RPA/RDA eller Machine Learning og monitoreringsløsninger.

Eftersom § 3, stk. 1, eksplicit hjemler "profilering" og definitionen af "beslutningsstøtte" i § 2, nr. 4, ikke gør, kan det bidrage til afklaring, hvis det præciseres, at begrebet "beslutningsstøtte" inkluderer profilering, da det vil skabe overensstemmelse mellem hjemlen i § 3, stk. 1, og definitionen.

Det fremgår af bemærkninger til de enkelte bestemmelsers s. 65, at grænsen mellem anvendelse af et AI-system til beslutningsstøtte og fuldautomatiserede afgørelser, skal afgøres af fremtidig retspraksis. Manglende afklaring kan lede til manglende retssikkerhed og klarhed i forhold til ansvar og rettigheder for kommunen som offentlig myndighed og de registrerede. I den anledning anføres det, at der både på området for databeskyttelse og AI er definitioner af, hvad menneskelig indgriben reelt består af fra præambelbetragtninger til EU-forordningerne, EU-domstolen samt via EDPB's udtalelser. EDPS har ligeledes offentliggjort en "Checklist on human intervention on automated decision-making (ADM)"[1], som kunne bruges som inspiration til udstede mere klare retningslinjer for myndigheder og organer.

Københavns Kommune bemærker, at lovforslaget giver mulighed for at træne på historiske og lukkede sager. Dette kan medføre et krav om ny oplysningspligt, hvis træningen med AI vil være til et nyt formål i forhold til det oprindelige formål med indsamlingen. Kommunen ser en række praktiske udfordringer heri, og opfordrer til, at myndighederne udsteder vejledning på området, så kommunens og de registreredes retsstilling er tydelig.

For så vidt angår Sundheds- og Omsorgsområdet har vi fået følgende input:

Det fremgår af s. 70 og 72, at lovforslaget laver en hjemmel til at behandle personoplysninger "det essentielle ved forståelsen af "opgavevaretagelse" er, at offentlige myndigheder og organer allerede ved hjemmel i anden lovgivning vil have ret til eller være forpligtede til at varetage denne opgave (s. 70) og "varetagelse af deres lovbestemte opgaver" (s. 72). Københavns Kommune varetager en lang række opgaver, hvor ikke alle er lovbestemte. Disse har typisk hjemmel i kommunalfuldmagten, men er, som anført, ikke reguleret af loven. Med denne hjemmel vil kommunen derfor ikke kunne udvikle AI-systemer på disse områder.

Kommunen forstår lovforslaget på den måde, at det kun er en hjemmel til udvikling og drift af AI-systemer, baseret på eget data. Eftersom opgaverne mellem regionerne og kommunerne er i kraftig

[1] 26-05-18_checklist-on-human-intervention-of-adm_en.pdf

udvikling, vil det være hensigtsmæssigt at fremtidssikre lovforslaget således at, man, af hensyn til volumen og kvalitet i datasæt, kan sammenlægge datasæt på tværs af regioner og kommuner i tilfælde af, at der skal løses en fælles opgave.

§ 3, stk. 2

Kommunen opfordrer til at tydeliggøre sammenhængen mellem § 1 og § 3, stk. 2, da § 1 giver indtryk af, at lovforslaget kun udgør en hjemmel for personoplysninger, der behandles med hjemmel i artikel 6, stk. 1, litra e, hvor § 3, stk. 2, gør det klart, at lovforslaget også er en hjemmel til at anvende AI på følsomme og andre kategorier af personoplysninger.

Konstruktionen hvor enhver enkelt ressortminister kan fastsætte specifikke foranstaltninger i bekendtgørelser, giver et potentielt modstridende retsgrundlag at arbejde på i kommunerne/hos offentlige myndigheder. F.eks. Ældreloven får tilføjet en bekendtgørelse, men serviceloven mangler en bekendtgørelse. Det vil udløse en kompleks retstilstand, hvor der mangler hjemmel på et overlappende område, som reelt vil betyde, at AI ikke kan anvendes på nogle af de to områder. Dette foreslås aktivt løst inden fremsættelse af lovforslaget. Man risikerer dermed alligevel at have et asymmetrisk og fragmenteret retligt landskab, hvilket ikke er formålet med lovgivningen.

Hensigtsmæssigheden af ordvalget "kan" skal overvejes, da man risikerer tilfælde, hvor behandlingen af følsomme personoplysninger er i igangsat, inden ressortministeren har fastsat de nævnte foranstaltninger. Når behandlingen først er igangsat – særligt hvis det indebærer ydelser fra en leverandør – kan den dataansvarlige risikere ikke at kunne ændre i AI-systemet i overensstemmelse med ressortministerens foranstaltninger. Dette vil betyde, at den dataansvarlige skal stoppe behandlingen og evt. udvikle et nyt system/funktion. Det er både ressourcetungt og spild af ressourcer at udvikle nye systemer/funktioner på bagkant. Nye krav til foranstaltninger fastsat på bagkant, kan også medføre, at den dataansvarlige sidder fast i en kontrakt, som den dataansvarlige ikke kan hæve uden væsentlige omkostninger, og den dataansvarlige risikere derfor at skulle betale for at system, som den dataansvarlige ikke må bruge.

Af lovforslagets specifikke bemærkninger på s. 74 fremgår det, at ressortministrene kan fastlægge foranstaltninger enten 1) i forhold til det konkrete system eller 2) en mere generel ramme for brug af AI-systemer inden for ressortområdet.

1) Tilgangen til specifikke systemer anses for at ville værende tidskrævende for myndighederne at vente på, ligesom det ville kræve en ikke uvæsentlig mængde af ressourcer at skulle sætte ressortministeren ind i, hvordan AI-systemet fungerer i en sådan grad, at ministeren kan fastlægge specifikke foranstaltninger.

2) I forhold til den generelle ramme kan dette ligeledes være svært, da foranstaltninger skal fastsættes på systemniveau, før de nedbringer risici, hvilket er derfor, at adresseringen af risici er den dataansvarliges ansvar i databeskyttelsesforordningen. Man kan også argumentere for, at det går imod den risikobaserede tilgang, som anvendes både i databeskyttelsesforordningen og NIS2, at man ikke tager stilling til de risici, som er forbundet med det konkrete system.

Det fremgår af bemærkningernes s. 45, at det skal overvejes, når et givent AI-system skal idriftsættes, om der er behov for at implementere yderligere foranstaltninger, herunder hvilke, og at det er derfor, at ministeren skal kunne fastsætte specifikke foranstaltninger til et givent AI-system efter behov. Kommunen undrer sig over, hvordan en sådan proces skal forløbe: skal de offentlige myndigheder henvende sig til den respektive ressortministre inden idriftsættelse for at få afklaret, om der skal fastsættes yderligere foranstaltninger? Hvis ja, hvor lang tid kan en offentlig myndighed forvente at vente på svar? Og hvad hvis brugen af AI-systemet vil gå på tværs af flere ressortområder? Kommunen er bekymret for, om den ekstra ventetid er hensigtsmæssig, også hvis ministeren skal tage stilling til foranstaltninger på systemniveau. Dette vil være forbundet med en vis mængde brug af ressourcer både for den pågældende minister, men også for den offentlige myndighed.

I bemærkningernes s. 30 fremgår det, at de offentlige myndigheder og organer aktivt skal tage stilling til, hvilke foranstaltninger der skal implementeres for at beskytte de registreredes rettigheder. På baggrund af bemyndigelsesbestemmelsen forstår kommunen dette som et blandet ansvarsområde. Dette faktum koblet sammen med ressortministerens mulighed, jf. "kan" (og ikke forpligtelse, jf. "skal"), for at implementere passende foranstaltninger bidrager ikke til en klarhed omkring ansvaret. Usikkerheden kan lede til, at kommunen kommer i en unødig "venteposition", mens det afklares, om ressortministeren ønsker at fastsætte specifikke foranstaltninger, særligt hvis det ikke offentliggøres, om ministeren ønsker det eller ej.

De problemer, som foranstaltningerne skal løse, kan også løses på systemniveau. Der kan derfor opstå situationer hvor de foranstaltninger, som ministeren fastsætter, ikke er nødvendige at implementere, da risikoen allerede er afhjulpet ved brug af andre

foranstaltninger. Det skal derfor overvejes, hvordan foranstaltningerne formuleres, så offentlige myndigheder undgår at blive pålagt at implementere unødvendige foranstaltninger.

Som lovforslaget - i forarbejderne - nævner, kan flere ressortministre gå sammen om at udstede en fælles bekendtgørelse i tilfælde, hvor et AI-system er tiltænkt anvendt på tværs af ressortområder (s.75). Kommunen håber, at Digitaliseringsstyrelsen får en fremtrædende koordinerende eller rådgivende rolle i denne proces.

§4, stk. 1

Der mangler i lovforslaget en klar definition af, hvor den dataansvarlige har hjemmel til at indskrænke de registreredes rettigheder. Dette er sammenholdt med nuværende praksis og vejledning fra både EDBP, herunder deres udtalelse i den henviste til udtalelse af 10/2020, og Datatilsynet. Hvis §4 fastholdes i den nuværende form vil det være afgørende at modtage konkret opdateret vejledning om, hvordan de dataansvarlige myndigheder skal forvalte denne bestemmelse fra Datatilsynets side samt i den kommende lov, hvilket vil være hensigtsmæssigt, hvis Digitaliseringsstyrelsen koordinerer i processen frem imod lovforslagets vedtagelse.

Endelig er det vurderingen af lovens formulering er i konflikt med princippet om retten til forklaring af individuel beslutningstagning jf. forordningen for kunstig intelligens artikel 86.

I bemærkningernes s. 45-46 fremgår det, at begrænsningen i de registreredes rettigheder skal være til et formål, som er omfattet af databeskyttelsesforordningens artikel 23. Dette anser kommunen som positivt. Tilføjelsen af afsnittet om komplicerede datastrukturer og at overholdelsen af de registreredes rettigheder kan være vanskelig og eller umuligt at overholde, virker i den kontekst afbalanceret og kan give indtrykket af at lægge vægt på de forkerte forhold. Endeligt opfordrer kommunen til, at den beføjelse som gives til ministrene, bliver brugt varsomt, da dataansvarlige kan ende i et rum med to modstridende love; Databeskyttelsesforordningen, der angiver et snævert rum for fravigelse af de registreredes rettigheder, og en bekendtgørelse, som giver offentlige myndigheder denne hjemmel. Bliver en potentiel afvisning med hjemmel i bekendtgørelsen bragt op på EU-niveau, står kommunen som dataansvarlig i en dårlig situation, hvor en national hjemmel og retsvildfarelse næppe vil frigøre kommunen for ansvar.

Til: Digitaliseringsstyrelsen – jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk, kahevi@digst.dk
Fra: Priway ApS, Stephan Engberg
Dato: 12. oktober 2026
Vedr.: Høringssvar til udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven) – høringsbrev af 14. september 2026

---

1. Sammenfatning

Lovforslaget bygger på en præmis, som ikke dokumenteres: at offentlige myndigheders adgang til at behandle identificerbare personoplysninger i AI-systemer er nødvendig for at opnå effektivitet, kvalitet og sikkerhed.

Vi mener, at det modsatte er tilfældet. Med eIDAS 2.0 er der i EU-retten etableret midler, som gør det muligt for borgeren at bidrage med kvalificerede, verificerbare oplysninger uden at blive identificeret eller sammenkørt på tværs af sammenhænge (Qualified Unlinkability). Når sådanne midler findes, følger det af databeskyttelsesforordningens artikel 25, stk. 1, at et design, der ikke anvender dem, skal begrundes – ikke omvendt.

Lovforslaget vender dette princip om. Det begrunder begrænsning af den registreredes rettigheder med hensynet til AI-systemets præcision, det skaber hjemmel til profilering uden krav om vurdering af mindre indgribende alternativer, og det adresserer efter egen angivelse ikke sikker håndtering af data.

Vi anbefaler, at lovforslaget omarbejdes som beskrevet i afsnit 7.

2. Det bærende princip: borgerens ret til midler til egenkontrol

Forordningen om det europæiske sundhedsdataområde (EU) 2025/327, artikel 71, etablerer borgerens kontrol som udgangspunkt for sekundær anvendelse af sundhedsdata. Medlemsstaterne kan kun fravige borgerens fravalg på kumulative betingelser, herunder at behandlingen er nødvendig (artikel 71, stk. 4, litra a), og at data "ikke kan tilvejebringes ad alternativ vej rettidigt og effektivt under tilsvarende betingelser" (artikel 71, stk. 4, litra b). Fravigelsen skal desuden være nødvendig og forholdsmæssig i et demokratisk samfund (artikel 71, stk. 5). Det er ikke et frit valg for borgeren at unddrage sig samfundsvigtige formål – men staten kan heller ikke tilsidesætte borgerens kontrol, når formålet kan opfyldes på anden måde.

Databeskyttelsesforordningens artikel 25, stk. 1, gør dette til et generelt princip. Den dataansvarlige skal – under hensyntagen til det aktuelle tekniske niveau – gennemføre foranstaltninger, der effektivt implementerer principperne om formålsbegrænsning og dataminimering, både på tidspunktet for fastlæggelse af midlerne og under selve behandlingen. Når et mindre indgribende middel er teknisk tilgængeligt, skal et mere indgribende design begrundes over for det.

eIDAS 2.0 (forordning (EU) 2024/1183), artikel 5a, stk. 16, leverer midlet. Den europæiske digitale identitetstegnebog skal muliggøre privatlivsfremmende teknikker, der sikrer ikke-sammenkobling, hvor attesteringen ikke kræver identifikation af brugeren. Midlet er dermed ikke hypotetisk; det er et EU-retligt krav, som Danmark skal gennemføre.

Tilsammen indebærer det, at **borgeren har ret til midler til egenkontrol, hvis borgeren vælger det.** Det er ikke et krav om, at alle skal anvende tegnebogen – brugen er frivillig, og ikke-brugere må ikke stilles ringere (eIDAS artikel 5a, stk. 15). Men det er et krav om, at muligheden stilles til rådighed, og at offentlige processer indrettes, så de kan modtage borgerens ikke-sammenkoblede bidrag.

Princippet forbedrer både sikkerhed og økonomi.

Sikkerhed. Qualified Unlinkability styrker sikkerheden på tre måder:

- *Risici skabes ikke.* Data, der ikke samles og sammenkøres, kan ikke lækkes, misbruges internt eller kræves udleveret. Risikoen fjernes i stedet for at blive forvaltet.
- *Forebyggende kontrol uden identifikation.* Med zero-knowledge-beviser kan der føres kontrol, før en ydelse eller adgang gives – f.eks. bevis for, at en person ikke er efterlyst, ikke er udelukket, eller opfylder en bestemt betingelse – uden at personen identificeres, og uden at kontrollen efterlader et sammenkørbart spor.
- *Betinget ansvarlighed.* Ansvarlighed opretholdes ved, at identifikation kun kan ske ved en dommerkendelse eller en formålsspecifik nødadgang ("break-the-glass") med lovbestemte betingelser. Det er en højere og mere kontrollerbar standard end en stående adgang til identificerbare data, der efterfølgende kontrolleres via logning.

Sikkerhed og retssikkerhed er dermed ikke modsætninger, men følger af samme arkitektur.

Økonomi. Forskellen handler om, hvem processerne indrettes efter. Når borgeren kan bidrage med præcis den oplysning, formålet kræver (f.eks. "opfylder kriterierne for ydelse X"), kan de digitale processer tilpasse sig borgernes reelle behov – efterspørgselsdrevet og på borgerens præmisser. Det er kendetegnet ved en økonomi, der løbende forbedres for at levere mere værdi for pengene. Det modsatte er en ordning, hvor borgeren skal tilpasse sig processer, der er fastlagt ovenfra. En sådan central styring sparer ikke penge ved at følge politiske prioriteringer; den gør samfundsøkonomien som helhed mindre effektiv, fordi den gør samfundet mindre tilpasningsdygtigt. Processer, der ikke kan tilpasse sig de behov, de skal betjene, forbedres ikke – de fastlåses. Lovforslaget måler effektivitet som tid sparet i den enkelte myndighed og overser denne samfundsøkonomiske omkostning.

3. Lovforslagets præmisser er ikke underbygget

Efter databeskyttelsesforordningens artikel 6, stk. 3, og Den Europæiske Unions Charter om Grundlæggende Rettigheder artikel 52, stk. 1, påhviler det lovgiver at godtgøre, at et indgreb er nødvendigt og forholdsmæssigt. Lovforslaget løfter ikke denne byrde.

3.1 Effektivitet antages, men dokumenteres ikke. Bemærkningerne pkt. 5 anfører, at myndighederne "kan opnå effektiviseringsgevinster og frigive tid til kerneopgaven", og at omkostningerne "vil blive opvejet" af gevinsterne. Der er ingen kvantificering, ingen basislinje og ingen sammenligning med alternativer, der ikke kræver behandling af identificerbare personoplysninger. Gevinsten opgøres udelukkende som tid sparet hos myndigheden; værdien for borgeren – og omkostningen for borgeren ved at miste kontrollen over egne data – indgår ikke.

3.2 Lovforslagets egne eksempler kræver ikke det, som lovforslaget giver hjemmel til. De nævnte

anvendelser – journalisering, mødeindkaldelser, tale-til-tekst, referatskrivning, dokumentationstjek og borgerrettede chatbots (pkt. 2.2.2.1 og pkt. 5) – forudsætter hverken profilering, træning på historiske sager eller begrænsning af den registreredes rettigheder.

3.3 Nødvendigheden er cirkulær. I pkt. 3 omdannes et ukvantificeret "potentiale" for effektivisering til "væsentlige samfundsinteresser", som herefter anvendes som grundlag for behandling af følsomme oplysninger efter artikel 9, stk. 2, litra g. Samtidig fastslår lovforslaget selv i pkt. 2.2.2.2, at "brugen af AI i sig selv ikke vil udgøre en væsentlig samfundsinteresse efter databeskyttelsesforordningens artikel 9, stk. 2, litra g". De to vurderinger er ikke forenelige.

3.4 Sikkerhed er udeladt. Lovforslaget anfører under principperne for digitaliseringsklar lovgivning: "Lovforslaget adresserer ikke princip 5 om sikker håndtering af data." Det vurderes ikke, at træning på historiske og lukkede sager og profilering på tværs af en myndigheds sager øger mængden af sammenkørbare personoplysninger og dermed angrebsflade, risiko for intern misbrug og risiko for tvungen udlevering. Det offentlige område omfatter væsentlige enheder efter NIS2-direktivet; en lov, der udvider den sammenkørbare databeholdning uden en sikkerhedsvurdering, svækker sikkerheden. Lovforslaget overser samtidig, at forebyggende kontrol og ansvarlighed kan opnås uden stående adgang til identificerbare data (afsnit 2).

4. Lovforslaget vender databeskyttelse gennem design om

Begrundelsen for § 4 (pkt. 3.1) er, at ministrene skal kunne fastsætte undtagelser til den registreredes rettigheder

> "for at sikre, at hensynet til den registreredes rettigheder ikke i alle tilfælde indebærer, at et AI-system vil skulle indrettes på en sådan måde, at disse kan iagttages, hvilket enten vil være umuligt eller vil svække AI-systemets præcision."

Det er det modsatte af artikel 25, stk. 1. Efter forordningen skal systemet indrettes, så rettighederne kan iagttages; efter lovforslaget skal rettighederne vige, hvis systemet ikke er indrettet til det. At rettigheder er "vanskelige" at opfylde, når personoplysninger først er indlejret i modelparametre (pkt. 2.3.2.1), er en følge af et designvalg – at indlejre personoplysninger – og ikke en teknisk nødvendighed.

Det bemærkes, at lovforslaget i forhold til høringsudkastet af 12. februar 2026 nu nævner artikel 25 blandt de regler, der skal overholdes (pkt. 2.2.2.1). Forpligtelsen nævnes, men lovforslagets konstruktion tager ikke højde for den.

5. Mangler i hjemmelsgrundlaget

5.1 § 4 – delegation af det, som ministeriet selv har afvist. I pkt. 2.3.2.1 vurderer ministeriet, at der "ikke foreligger et tilstrækkeligt grundlag for at etablere en generel databeskyttelsesretlig hjemmel for undtagelse til den registreredes rettigheder". Alligevel overlades det i § 4 til ressortministrene at fastsætte sådanne undtagelser ved bekendtgørelse – efter pkt. 2.3.2.1 også for hele sektorer. Artikel 23, stk. 2, kræver, at en begrænsning sker ved en lovgivningsmæssig foranstaltning, der indeholder specifikke bestemmelser om bl.a. formål, kategorier af oplysninger, begrænsningens omfang, garantier og risici. En generel bemyndigelse

opfylder ikke dette.

5.2 Statistik og berigelse er to forskellige ting – og berigelse skaber nye personoplysninger. Lovforslaget skelner ikke mellem to grundlæggende forskellige former for sekundær anvendelse:

- *Statistik på transaktionsdata*. Optællinger, fordelinger og tendenser over eksisterende sagsdata tilføjer ikke nye oplysninger om den enkelte. Sådan statistik giver stort set samme resultat, uanset om den gennemføres på identificerbare data med dataminimering eller med Qualified Unlinkability. Forskellen er den regulatoriske byrde: Med Qualified Unlinkability er kravet alene at begrænse antallet af attributter til det, der er nødvendigt for at opretholde ikke-sammenkoblingen. Når samme resultat kan opnås med mindre indgreb og mindre byrde, er det identificerede alternativ hverken nødvendigt eller forholdsmæssigt.
- *Berigelse*. Enhver kombination af personoplysninger, der ikke sker under borgerens egen kontrol på klientsiden med Qualified Unlinkability, skaber nye personoplysninger – f.eks. ved profilering, træning eller beslutningsstøtte: slutninger, scorer, risikovurderinger og kategoriseringer, som ikke eksisterede før.

Lovforslaget anfører, at det "ikke vil fungere som en hjemmel til at behandle nye personoplysninger" (pkt. 2.2.2.1). Samtidig erkender det, at profilering kan resultere i særlige kategorier af personoplysninger, som "kan udledes af personoplysninger, der ikke i sig selv udgør særlige kategorier" (pkt. 2.2.2.2). Profilering er netop frembringelse af nye personoplysninger. Lovforslaget giver dermed hjemmel til det, det angiver ikke at give hjemmel til.

Berigelse er sekundær anvendelse. Lovforslaget betegner selv træning på historiske og lukkede sager som "viderebehandling" (pkt. 2.2.2.3), og forordningen om det europæiske sundhedsdataområde nævner udtrykkeligt "træning, afprøvning og evaluering af algoritmer, herunder … AI-systemer" som formål for sekundær anvendelse (artikel 53, stk. 1, litra e, nr. ii). Betingelsen i artikel 71, stk. 4, litra b, om, at data ikke kan tilvejebringes ad alternativ vej under tilsvarende betingelser, gælder netop sådan anvendelse.

Frembringelse af nye personoplysninger kræver et selvstændigt, klart og præcist retsgrundlag for netop den berigelse – med angivelse af formål, hvilke oplysninger der kobles, og hvilke nye oplysninger der skabes. Det giver lovforslaget ikke, og det kan en generel hjemmel ikke give.

5.3 Træning uden forenelighedstest. Efter pkt. 2.2.2.3 er det et udtrykkeligt formål, at myndighederne "ikke vil skulle foretage en forenelighedstest i henhold til databeskyttelsesforordningens artikel 6, stk. 4", før historiske og lukkede sager anvendes til træning. Det er netop i forenelighedstesten, at fornødne garantier som pseudonymisering og kryptering indgår. Lovforslaget fjerner dermed det sted i processen, hvor mindre indgribende alternativer skulle være overvejet.

5.4 § 3, stk. 2, er en mulighed, ikke en pligt. Bemærkningerne fastslår, at der "ikke etableres en generel forpligtelse" til at fastsætte foranstaltninger for følsomme oplysninger og oplysninger om strafbare forhold, og at eksisterende garantier f.eks. kan følge af "individuelle dataansvarliges databehandlingspolitikker". Det er ikke "passende og specifikke foranstaltninger" i artikel 9, stk. 2, litra g's forstand.

5.5 Profilering uden afgrænsning. § 3 giver hjemmel til "blandt andet" profilering for alle offentlige myndigheder og organer, uden afgrænsning af formål, kategorier af oplysninger eller betingelser.

Datatilsynets praksis, som lovforslaget henviser til, kræver et klart og præcist retsgrundlag netop for indgribende behandling. En generel hjemmel, der dækker alt fra referatskrivning til profilering, opfylder ikke dette krav for den indgribende del.

6. Midlerne findes – og er tilbudt demonstreret

eIDAS 2.0 er beviset for, at ikke-sammenkoblede midler er det aktuelle tekniske niveau: EU-lovgiver har gjort dem til et krav for den europæiske digitale identitetstegnebog.

Priway ApS ansøgte om deltagelse i Datatilsynets og Digitaliseringsstyrelsens regulatoriske sandkasse med det formål at demonstrere lovlige, sikre alternativer i situationer, hvor AI ellers ville få adgang til personoplysninger, og at give begge myndigheder mulighed for at verificere dette. Ansøgningen blev afslået den 4. juni 2026 (Datatilsynets j.nr. 2026-211-5183) uden konkret begrundelse ud over en henvisning til de generelle udvælgelseskriterier.

Den 5. juni 2026 (Digitaliseringsstyrelsens sag 2859208) opfordrede vi Digitaliseringsstyrelsen til at tilpasse lovforslaget til det aktuelle tekniske niveau, og vi tilbød den 24. juni 2026 at påvise lovlige alternativer for enhver use case, styrelsen måtte rejse. Styrelsen henviste den 25. juni 2026 til den kommende høring.

Tilbuddet står ved magt.

7. Forslag til ændringer

1. **Pligt til alternativvurdering (ny § 3, stk. 2).** Før en myndighed anvender et AI-system til profilering eller på oplysninger omfattet af artikel 9 eller 10, skal myndigheden dokumentere, om formålet kan opfyldes uden behandling af identificerbare personoplysninger, herunder ved ikke-sammenkoblede attesteringer efter eIDAS 2.0, zero-knowledge-baseret forebyggende kontrol og betinget identifikation ved dommerkendelse eller formålsspecifik nødadgang. Kan formålet opfyldes sådan, skal det ske.
2. **Borgerens valg af egenkontrol.** Hvor borgeren har valgt at bidrage ikke-sammenkoblet via den europæiske digitale identitetstegnebog, må myndigheden ikke anvende identificerbare oplysninger om borgeren til udvikling eller træning af AI-systemer. Ikke-brugere må ikke stilles ringere.
3. **§ 4 udgår.** Begrænsninger af den registreredes rettigheder fastsættes i sektorlovgivningen med det indhold, artikel 23, stk. 2, kræver – og aldrig med henvisning til AI-systemets præcision.
4. **§ 3, stk. 2, gøres obligatorisk** ("skal fastsætte") for oplysninger omfattet af artikel 9 og 10 og for profilering.
5. **Statistik og berigelse adskilles.** Statistik på transaktionsdata skal ske med Qualified Unlinkability eller på anonymiserede data, hvor det giver samme resultat. Berigelse – herunder profilering og træning på historiske og lukkede sager – anerkendes som frembringelse af nye personoplysninger og behandles som sekundær anvendelse. Forenelighedstesten bevares, og berigelse kræver et selvstændigt retsgrundlag i sektorlovgivningen og må kun ske på identificerbare data, hvis formålet ikke kan opfyldes med ikke-sammenkoblede data under tilsvarende betingelser (jf. artikel 71, stk. 4, litra b).
6. **Sikkerheds- og gevinstvurdering.** Før fremsættelse udarbejdes en vurdering efter princip 5 for digitaliseringsklar lovgivning og en dokumenteret gevinstberegning, der sammenligner med

ikke-sammenkoblede alternativer.

8. Vejen ud: fra datamaksimering til valg

Kravet om dataminimering har gældt siden databeskyttelsesdirektivet fra 1995 (direktiv 95/46/EF, artikel 6, stk. 1, litra c), der krævede, at oplysninger skal være "tilstrækkelige, relevante og ikke omfatte for meget". Dansk offentlig digitalisering har ikke desto mindre udviklet sig i den modsatte retning: en selvforstærkende datamaksimering bygget på CPR-nummeret som gennemgående nøgle. Resultatet er en betydelig teknologisk gæld, øget usikkerhed og ineffektivitet – både i den offentlige sektor og i den private sektor, som gennem den offentlige sektors administrative krav er tvunget til at indrette sig efter samme model.

Det er ikke let at vende denne udvikling. Men AI-transformationen gør det både nødvendigt og – med et design baseret på Qualified Unlinkability – muligt.

Vejen ud er gradvis og drives af borgerne: ved at give dem reelle midler og retten til at tage kontrollen. Ser borgeren ikke fordelen, vælger borgeren det fra. Pointen er, at når der findes reelle midler til ikke-sammenkoblede transaktioner og ydelser, er begge veje et valg. Uden sådanne midler findes der ingen mekanisme, der over tid kan gøre økonomien mere effektiv.

Muligheden for at håndhæve valg gennem kontrol over egne data virker i både den offentlige og den private sektor. Den er derfor ikke et politisk-ideologisk valg, men alene respekt for de grundlæggende principper, som både EU-retten og et velfungerende samfund hviler på.

Lovforslaget bør derfor ikke blot ændres på de punkter, der er nævnt i afsnit 7. Det bør indgå i en plan for, hvordan den offentlige sektor gradvist bevæger sig fra datamaksimering til borgerstyret kontrol – med AI som anledningen og Qualified Unlinkability som midlet.

Vi deltager gerne i en dialog om ændringerne og om en demonstration af de tekniske løsninger.

Med venlig hilsen

Stephan Engberg
Priway ApS
Stengårds Allé 33D, 2800 Kgs. Lyngby
Stephan.Engberg@Priway.EU · +45 2834 0404

Til: jonmei@digst.dk, kahevi@digst.dk, emimol@digst.dk, leaomd@digst.dk
Fra: Karen Englev (keng@rigsrevisionen.dk)
Titel: SV: Høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger
Sendt: 09-10-2026 09:34
Bilag: image001.png;

Til Digitaliseringsstyrelsen

Digitaliseringsstyrelsen har den 14. september 2026 sendt udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven) i høring.

Ministeriernes forpligtelse til at høre Rigsrevisionen er fastlagt af rigsrevisorloven, §§ 7 og 10 (lovbekendtgørelse nr. 101 af 19. januar 2012), og angår revisions- og/eller regnskabsforhold, der kan have betydning for Rigsrevisionens opgaver.

Vi har gennemgået lovforslaget og kan konstatere, at det ikke omhandler revisions- eller regnskabsforhold i staten eller andre offentlige virksomheder, der revideres af Rigsrevisionen.

Vi har derfor ikke behandlet henvendelsen yderligere.

Med venlig hilsen

Karen Englev
Fuldmægtig

FOLKETINGET
RIGSREVISIONEN

Landgreven 4
DK-1301 København K

Tlf. +45 33 92 84 00
Dir.+45 33 92 84 45
keng@rigsrevisionen.dk

www.rigsrevisionen.dk

Læs om Rigsrevisionens behandling af personoplysninger her

Fra: Jonathan Kirkegaard Meijer <jonmei@digst.dk>
Sendt: 14. september 2026 10:41
Emne: Høring om forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger

Kære høringspart

Digitaliseringsstyrelsen anmoder hermed om eventuelle bemærkninger til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Eventuelle høringssvar bedes fremsendt via e-mail til jonmei@digst.dk, kahevi@digst.dk, emimol@digst.dk og leaomd@digst.dk senest kl. 12:00 den 12. oktober 2026.

Høringsmaterialet kan også ses på Høringsportalen via følgende link: https://hoeringsportalen.dk/Hearing/Details/71477 hvor modtagne høringssvar også vil blive gjort tilgængelige.

Med venlig hilsen

Digitaliserings-
styrelsen

Jonathan Meijer
Fuldmægtig
Kontor for AI, analyse og inklusion

T 2485 9061
E jonmei@digst.dk

_____

www.digst.dk

Du bedes venligst være opmærksom på, at Digitaliseringsstyrelsen ved modtagelsen af din meddelelse behandler de personoplysninger om dig, der fremgår af beskeden. Dette sker som led i Digitaliseringsstyrelsens myndighedsudøvelse. Du kan læse mere om, hvordan Digitaliseringsstyrelsen behandler dine personoplysninger, og hvilke rettigheder du har som registreret mv., i styrelsens privatlivspolitik https://digst.dk/om-os/privatlivspolitik/

7. oktober 2026

Rådet for Digital Sikkerhed

Høringssvar

Digitaliseringsministeriets udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven) (frist 12.10.26)

I henhold til Digitaliseringsministeriets høringsskrivelse af 14. september 2026 fremsendes dette høringssvar til følgende: jomei@digst.dk, kahevi@digst.dk, emimol@digst.dk og leaomd@digst.dk.

Rådet for Digital Sikkerhed takker for at blive inddraget i høringen af lovudkastet om AI-hjemmelsloven, idet det bemærkes, at vi også afgav høringssvar på det oprindelige lovudkast fra februar 2026.

Rådet er fortsat enige i intentionen om at skabe klar hjemmel til udvikling og anvendelse af allerede indsamlede personoplysninger til udvikling og anvendelse af AI-systemer i det offentlige. Efter Rådets vurdering er der dog fortsat flere forhold, som påkalder sig særlig opmærksomhed:

1. Hvad kan AI-systemerne bruges til?

I det første høringssvar gav Rådet udtryk for, at en kommende lov mere eksplicit bør forholde til, hvor man skal sætte grænsen mellem 'beslutningsunderstøttelse' og egentlig sagsbehandling, der har konsekvenser for borgeren.

Det nye høringsudkast adresserer problemstillingen, idet det på den ene side tydeliggøres i selve lovteksten, at beslutningsstøtte omfatter *"…forslag eller anbefaling til afgørelser eller væsentlige tiltag overfor den registrerede, og som en fysisk person inddrager i den samlede faglige vurdering…".* Endvidere præciserer lovteksten, at udviklede AI-systemer, kan anvendes til *"…blandt andet evaluering af bestemte personlige forhold vedrørende en borger (profilering)…".*

På den anden side præciseres det i lovbemærkningerne s. 19, at kravet til menneskelig involvering (som nu fremgår af lovtekstens § 3) *"…blandt andet kunne understøttes ved at identificere, hvem der har beslutningskompetencen ved brug af AI-systemet, fastlægge hvordan afvigelser fra AI-systemets anbefalinger og forslag håndteres og dokumenteres, samt sikre relevant logning af anvendelsen af AI-systemet. Sådanne procedurer kan bidrage til at sikre og dokumentere, at den menneskelige involvering er reel og ikke alene udgør en formalitet. Det bemærkes dog, at sådanne understøttende procedurer ikke i sig selv er et krav efter denne lovgivning. Det afgørende er fortsat, om den person, der har beslutningskompetencen, foretager en reel og selvstændig vurdering af AI-systemets anbefaling eller forslag."*

De angivne præciseringer er selvsagt velkomne. Det er kort sagt blevet tydeligere, hvad hensigten er med lovforslaget, og hvad den generelle hjemmel kan anvendes til af det offentlige.

Det bør dog fortsat overvejes at stille som krav, at den offentlige forvaltning ved meddelelse til borgeren om en afgørelse eller anden form for indvirkende tiltag, der hidrører fra AI, ledsager henvendelsen med en bemærkning om, at den netop er baseret på AI-anvendelse. Lovbemærkningernes 'anbefalinger' til dokumentation for menneskelig involvering er primært målrettet de interne procedurer, med risiko for, at borgeren bliver tabt i forståelsen af, hvilke informationer og overvejelser, det offentlige organ selvstændigt og ved menneskelig involvering måtte have lagt til grund for henvendelsen. Forvaltningslovens begrundelseskrav bør også iagttages i denne sammenhæng, eftersom grænsefladen mellem beslutningsstøtte, der kan føre til indvirkende henvendelser, og egentlige afgørelser ikke er krystalklar.

Som nævnt i Rådets første høringsbrev bør det derfor overvejes, at det offentlige bliver forpligtet til at oplyse om 1. AI-systemets anbefaling / evaluering i den givne sag 2. Forvaltningens overvejelser på baggrund af anbefalingen / evalueringen 3. Forvaltningens begrundelse for henvendelsen / begrundede afgørelse efter de almindelige forvaltningsretlige principper.

Den fornødne præcisering understreges af, at der ikke er etableret en fast definition af AI anvendt i forbindelse med beslutningsunderstøttelse og evaluering af personlige forhold - jf. også bemærkningerne i udkastet om, at det *"…må forventes at fremtidig retspraksis vil bidrage til præcisere, hvilken grad af menneskelig involvering, der kræves for, at anvendelsen af et AI-system vil kunne anses som beslutningsunderstøttelse…"* (s. 68).

2. Personoplysninger, der kan anvendes til udvikling af AI-modeller

Bemærkningerne til det oprindelige lovudkast efterlod en uklarhed om, hvorvidt en myndighed kan indsamle nye personoplysninger, der alene foretages med henblik på udvikling af AI-systemer - og ikke i første omgang er indhentet som led i den konkrete sagsbehandling, som myndigheden i henhold til lovgivningen varetager.

Det oprindelige lovudkast efterlod også en uklarhed om muligheden for videregivelse af allerede indsamlede personoplysninger til udvikling af AI, hvor det fremgik af de daværende lovbemærkninger, at loven ikke vil "... adressere eventuelle generelle problemstillinger for myndigheder i den offentlige forvaltning i forhold til deres mulighed for at videregive personoplysninger til en anden offentlig myndighed...".

Rådet bemærker, at det i lovbemærkningerne nu er præciseret, at AI-hjemmelsloven, hverken vil give det offentlige mulighed for *"…at indsamle yderligere personoplysninger, end dem som myndigheden allerede efter gældende ret lovligt må indsamle og behandle til brug for AI-systemet…*" eller "*…give hjemmel til, at offentlige myndigheder og organer kan videregive personoplysninger til andre offentlige myndigheder og organer.*" (s. 71-72).

Rådet hilser præciseringen velkommen, men vil foretrække at det indføjes i selve lovteksten, at det offentliges adgang til at indhente eller videregive personligoplysninger reguleres i databeskyttelsesforordningen, og at AI-hjemmelsloven ikke tilføjer videre hjemmel.

Det bør i den forbindelse også overvejes, at de person-karakteristika, som et AI-system kan genere (profileringsdata) i sig selv kan opfattes som nye personoplysninger om en borger. Her bør lovudkastet adressere, at ej heller sådanne oplysninger kan videregives uden hjemmel i databeskyttelsesforordningen. Rådet er opmærksom på, at lovforslagets § 3, stk. 2 giver ressortministre mulighed for at fastsætte foranstaltninger til beskyttelse af særlige kategorier af personoplysninger, der dannes via såkaldt 'AI-deduktion', men vil foretrække, at spørgsmålet om videregivelse af sådanne oplysninger adresseres tydeligere.

3. Er der skabt den fornødne sikkerhed for, at persondata ikke opsamles hos en udbyder af store AI-systemer, der lægges til grund for træning af nye lokale og specialiserede AI-systemer i det offentlige (tredjelandsoverførsler)?

Også af det nye lovudkast fremgår det, at loven ikke adresserer problemstillinger, der er relateret til tredjelandsoverførsler (s. 7). Rådet skal derfor blot gentage sin bemærkning fra den oprindelige høring:

I lyset af debatten om digital uafhængighed (og den generelle debat om cybersikkerhed, udviklingen i risikobilledet, digitale rettigheder og digital innovation i Europa) bør lovforslaget netop adressere tredjelandsproblematikken. Det kan ske ved, at de AI-modeller, som loven giver danske offentlige myndigheder øgede mulighed for at udvikle, som udgangspunkt alene trænes på grundlag af AI-træningsmetoder, der ikke samtidig medfører dataoverførsel mellem den specialiserede danske model og eventuelt store træningsmodeller, som måtte blive anvendt som træningsfundament. Hvis lovudkastet ikke adresserer tredjelandsproblematikken relateret til store træningsmodeller, skal de offentlige myndigheder finde hjemmel til denne overførsel i databeskyttelsesforordningens kapitel V, hvilket vil være byrdefuldt for myndighederne.

Det er muligt at visse nye offentlige AI-modeller kun kan udvikles ved at den omtalte dataoverførsel finder sted. Derfor bør de under alle omstændigheder stilles som krav, at offentlige organer (jf. lovforslagets definition) i videst mulige omfang anvender privatlivsfremmende teknologier i udvikling og den løbende vedligeholdelse af AI-modellerne.

4. Kan de registrerede fastholde deres grundlæggende rettigheder til databeskyttelse?

Rådet erindrer om, at borgernes rettigheder i tilknytning til beskyttelse af personoplysninger (jf. art. 8 i EU chartret), der indgår i træningen af en AI-model, kun meget vanskeligt og omkostningsfuldt kan imødekommes.

Det er derfor afgørende, at den offentlige forvaltning er forpligtet til gennemsigtighed, hvad angår AI-modellernes funktionsmåde, deres anvendelsesformål og -afgrænsning, hvilke typer persondata, der er anvendt i udviklingen samt ikke mindst, hvordan den enkelte borgers persondata fortsat vil være beskyttet mod datalæk, misbrug og uintenderet profilering. Yderligere er det vigtigt at

understrege, at forslaget giver hjemmel for den offentlige forvaltning, men at forvaltningen stadig efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, skal foretage en nødvendighedsvurdering. Ligeledes er det vigtigt, at den offentlige forvaltning gennemfører risikovurderinger og evt. konsekvensanalyser, hvor de registreredes risiko er i fokus.

Endelig er det vigtigt at understrege, at lovinitiativets præmis om menneskelig involvering i såvel sikringen af ansvarlige AI-modeller som i forholdet mellem forvaltning og borger bør være en ledetråd for den fremtidige AI udvikling i det offentlige.

Afslutningsvist er det vigtigt at bemærke, at det forhold, at der etableres hjemmel for den offentlige forvaltning, ikke sætter de persondataretlige regler ud af kraft. Den offentlig forvaltning skal derfor iagttage præcis de samme databeskyttelsesregler, som de har været pålagt siden databeskyttelsesforordningen blev vedtaget.

Rådet skal i tilknytning hertil og i lyset af fx EU Domstolens afgørelse C-175/20[1] bemærke, at loven giver en meget bred hjemmel til en meget bred gruppe af aktører. Rådet er ikke overbevist om at en så bred hjemmel udgør "klare og fremtidssikre lovgivningsmæssige rammer for offentlige myndigheders anvendelse af kunstig intelligens" (s. 5). Rådet vil i den forbindelse henvise til, at Digitaliseringsministeriet bør lægge stor vægt på de indkomne høringssvar, herunder navnlig svarene fra Datatilsynet og Institut for Menneskerettigheder.

[1] Se fx https://www.juridicainternational.eu/article_full.php?uri=2024_33_data-driven_public_administration_and_the_gdpr_seeing_the_court_of_justice_s_judgement_in_ca

Ældre Sagen

Digitaliseringsstyrelsen
jonmei@digst.dk, emimol@digst.dk, leaomd@digst.dk og kahevi@digst.dk

8. oktober 2026

Ældre Sagen
Snorresgade 17-19
2300 København S

Tlf. 33 96 86 86
www.aeldresagen.dk
aeldresagen@aeldresagen.dk

Høringssvar vedr. forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Ældre Sagen takker for muligheden for at afgive høringssvar vedrørende forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven).

Ældre Sagen anerkender behovet for et tydeligt og tidssvarende retsgrundlag for offentlige myndigheders anvendelse af kunstig intelligens, ligesom vi anerkender, at kunstig intelligens kan bidrage til bedre ressourceudnyttelse og understøtte myndighedernes opgavevaretagelse herunder nedbringe sagsbehandlingstider.

Efter Ældre Sagens opfattelse giver lovforslaget imidlertid en meget bred og generel hjemmel til udvikling og anvendelse af AI-systemer på tværs af den offentlige sektor, på bekostning af en række retssikkerhedsgarantier.

Overordnet retssikkerhedsmæssig ubalance
Lovforslaget hjemler et behandlingsgrundlag for myndighedernes anvendelse af AI, men indeholder kun få eksplicitte garantier for borgere, der bliver genstand for AI-understøttet sagsbehandling. Dette er særligt problematisk, fordi AI-systemer kan tilsidesætte grundlæggende forvaltningsretlige principper.

Det er derfor efter Ældre Sagens vurdering ikke tilstrækkeligt at henvise til, at de almindelige forvaltningsretlige regler fortsat gælder. Lovforslaget introducerer en ny teknologisk beslutningsstruktur, som kræver særskilte og lovfæstede retssikkerhedsgarantier, der ikke fremgår af lovforslaget.

Beslutningsstøtte og risiko for reelt automatiserede afgørelser
Lovforslaget bygger på en forudsætning om, at AI-systemer alene skal anvendes som beslutningsstøtte. Efter Ældre Sagens vurdering er denne forudsætning imidlertid ikke tilstrækkeligt understøttet af lovforslagets indhold.

Når AI-systemer kan generere forslag eller anbefalinger til afgørelser er der en reel risiko for, at disse vurderinger i praksis får afgørende betydning for

sagsbehandlerens beslutning. Dermed kan den menneskelige vurdering gradvis reduceres til en formel kontrol af AI-systemets anbefaling.

Ældre Sagen finder derfor, at loven bør præcisere, hvilke krav der skal være opfyldt for, at den menneskelige beslutningskompetence kan anses for reel, og dermed hvilken grad af menneskelig involvering der kræves for, at anvendelsen af et AI-system kan anses som beslutningsstøtte efter lovforslaget og ikke fuldautomatiske afgørelser. Det bør blandt andet sikres, at sagsbehandleren aktivt og selvstændigt skal vurdere sagens faktiske og retlige omstændigheder og ikke blot tilslutte sig systemets anbefaling.

Borgernes rettigheder skal beskyttes
Ældre Sagen finder det særdeles betænkeligt, at lovforslaget giver mulighed for ved bekendtgørelse at begrænse centrale rettigheder efter databeskyttelses-forordningen.

Der er tale om rettigheder, som udgør helt centrale retssikkerhedsgarantier for borgerne og er afgørende for muligheden for at forstå, kontrollere og eventuelt påklage myndigheders behandling af personoplysninger og afgørelser.

Jo større betydning AI får for den offentlige myndighedsudøvelse, desto stærkere bør de registreredes rettigheder beskyttes. Lovforslaget bevæger sig efter Ældre Sagens opfattelse i den modsatte retning ved at åbne mulighed for administrative begrænsninger af disse grundrettigheder.

Ældre Sagen finder derfor, at eventuelle begrænsninger af borgernes rettigheder alene bør kunne ske ved lov og ikke ved administrative forskrifter.

Behov for generelle og ensartede retsgarantier
Lovforslaget er af generel karakter og gælder på tværs af sektorer. Efter Ældre Sagens opfattelse bør dette ledsages af nogle generelle retsgarantier, som gælder for alle borgere uanset forvaltningsområde.

Hvis beskyttelsesforanstaltninger og retsgarantier overlades til de enkelte ministerområder og myndigheder, er der risiko for betydelige forskelle i borgernes beskyttelse.

Risiko for bias, diskrimination og systematiske fejl
Lovforslaget anerkender risikoen for bias og diskrimination, men giver efter Ældre Sagens opfattelse ikke tilstrækkelige svar på, hvordan disse risici skal håndteres.

Historiske data afspejler eksisterende praksis. Hvis denne praksis indeholder fejl, vil AI-systemer kunne reproducere eller forstærke disse i stor skala. Fejl, som tidligere berørte enkelte sager, kan dermed få systemisk karakter. Samtidig har Folketingets Ombudsmand gennem en række sager peget på udfordringer med offentlige digitale løsninger og deres overholdelse af forvaltningsretlige krav.

Ældre Sagen frygter tillige, at der på en lang række forvaltningsområder, herunder ældreområdet, er omsorgsmæssige, relationelle og individuelle hensyn, der ofte ikke vil være nedskrevet og derfor ikke vil indgå i datagrundlaget. Der er dermed en potentiel risiko for, at væsentlige skønsmæssige forhold ikke vil indgå i den beslutningsstøttede sagsbehandling og dermed heller ikke i afgørelsen.

Ældre Sagen frygter, at det vil betyde, at det forvaltningsretlige skøn vil blive udhulet, og at den individuelle og konkrete vurdering, der skal foretages efter forvaltningsretten, ikke vil blive foretaget.

Ældre Sagen finder derfor, at loven bør indeholde krav om test for bias og diskrimination, dokumentation af datagrundlag og modeller, uafhængig kontrol og revision samt offentlig rapportering om fejl, afvigelser og risici.

Retssikkerhed og tillid til den offentlige sektor
Den offentlige sektors anvendelse af kunstig intelligens forudsætter en høj grad af offentlig tillid. Anvendelsen af AI skal ske med respekt for borgernes retssikkerhed og grundrettigheder.

Ældre Sagen finder, at lovforslaget i sin nuværende form giver offentlige myndigheder omfattende nye muligheder for at udvikle og anvende AI-systemer uden samtidig at etablere tilsvarende stærke retssikkerhedsgarantier for borgerne.

Lovforslaget flytter efter Ældre Sagens opfattelse balancen mellem effektivisering og retssikkerhed i en problematisk retning. Der er risiko for, at den teknologiske udvikling kommer til at ske for hurtigt og på bekostning af de retssikkerhedsmæssige værn, der skal beskytte borgerne.

Ældre Sagen opfordrer derfor til, at centrale retssikkerhedsgarantier fastsættes direkte i loven, at borgernes rettigheder ikke kan begrænses administrativt, og at der indføres krav til den menneskelige involvering og forebyggelse af diskrimination ved anvendelsen af kunstig intelligens i den offentlige sektor og ved offentlig myndighedsudøvelse.

Venlig hilsen

Michael Teit Nielsen
Vicedirektør

Aalborg Kommune, AI-Fællesskabet // Informationssikkerhed
Danmarksgade 17A, 9000 Aalborg

Digitaliseringsstyrelsen
Landgreven 4
1301 København K

Aalborg Kommune
AI-Fællesskabet
Danmarksgade 17A
9000 Aalborg
+4525201722

Sagsnr.: 2026-066763

Mandag 8-15
Tirsdag 8-15
Onsdag 8-15
Torsdag 8-17
Fredag 8-15
Weekend lukket

12.10.2026

Høringssvar fra Aalborg Kommune

Aalborg Kommune takker for muligheden for at afgive bemærkninger til lovforslaget. Kommunen støtter overordnet formålet om at skabe et tydeligere og mere ensartet databeskyttelsesretligt grundlag for offentlige myndigheders udvikling og anvendelse af AI-systemer. En generel hjemmel kan bidrage til at reducere den nuværende usikkerhed omkring anvendelse af AI i offentlige myndigheder.

Aalborg Kommune finder samtidig, at lovforslagets brede og tværgående karakter skaber behov for yderligere præcisering og praktisk vejledning. Kommunens bemærkninger nedenfor er afgrænset til de spørgsmål, der har særlig betydning for kommunernes databeskyttelsesretlige compliance i forbindelse med anvendelse af AI.

1. Lovforslagets anvendelsesområde og forholdet til følsomme personoplysninger

Aalborg Kommune forstår lovforslagets § 3, stk. 1 således, at det skal udgøre det generelle nationale supplerende retsgrundlag for offentlige myndigheders udvikling og anvendelse af AI-systemer ved behandling af personoplysninger som led i myndighedsudøvelse. Kommunen noterer i den forbindelse, at lovforslaget efter bemærkningerne skal anses for at udgøre det supplerende retsgrundlag til behandling af både almindelige personoplysninger efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, følsomme personoplysninger efter artikel 9, stk. 2, litra g, og oplysninger om strafbare forhold efter artikel 10.

Aalborg Kommune er enig i lovforslagets beskrivelse af Datatilsynets praksis, hvorefter behovet for et særligt klart og præcist supplerende retsgrundlag opstår ved indgribende behandling af personoplysninger med kunstig intelligens, herunder ved beslutningsstøtte og andre anvendelser, som kan have væsentlig betydning for de registrerede. Kommunen er samtidig enig i, at der for en række mindre indgribende anvendelser af kunstig intelligens ofte allerede vil kunne findes et tilstrækkeligt supplerende retsgrundlag i den eksisterende sektorlovgivning.

Efter en del dialog under høringsperioden med andre kommuner og KL er det blevet klart, at der findes forskellige fortolkninger af, hvad lovforslagets § 3, stk. 1 giver supplerende retsgrundlag til i sig selv, og hvad der er givet bemyndigelse til ressortministerierne til at fastsætte i bekendtgørelser efter lovforslagets § 3, stk. 2.

På baggrund af dialogen er det Aalborg Kommunes opfattelse, at lovforslaget skal fortolkes i overensstemmelse med ovenstående indledningsvise beskrivelse. Altså at lovforslaget i sig selv skal fungere som det supplerende retsgrundlag for både behandling af almindelige og følsomme personoplysninger samt oplysninger om strafbare forhold.

Mange AI-projekter i kommunerne og andre myndigheder vil omfatte behandling af både almindelige og følsomme personoplysninger, og det vil ofte ikke være muligt at undgå behandling af følsomme personoplysninger som led i den almindelige opgavevaretagelse.

For den fremtidige anvendelse og fortolkning af loven som supplerende retsgrundlag til anvendelse og udvikling af kunstig intelligens i offentlige myndigheder er det derfor af afgørende betydning, at lovforslaget og bemærkningerne gør det helt klart, om ovenstående fortolkning af korrekt, eller om der skal anlægges en anden fortolkning af, hvad lovforslaget giver supplerende retsgrundlag til.

Hvis der efter lovens ikrafttræden fortsat eksisterer stor fortolkningstvivl om, hvilket supplerende retsgrundlag, som loven reelt giver, vil den hermed forbundne juridiske usikkerhed være en stor ulempe i arbejdet med fremtidige AI-projekter, fordi der i dag er et stort behov for at sikre, at lovgivningen fortolkes ensartet på tværs af myndigheder. Det ses også i bemærkningerne, at det er et af lovforslaget formål at udviske den uensartede fortolkning af retstilstanden i dag, og det formål er der en risiko for ikke opfyldes, hvis fortolkningstvivlen ikke fjernes i det endelige lovforslag.

Aalborg Kommune anbefaler derfor, at det i det endelige lovforslag eller tilhørende vejledningsmateriale præciseres hvilket selvstændig supplerende retsgrundlag, som loven er tiltænkt i forhold til behandling af følsomme personoplysninger efter artikel 9 og oplysninger om strafbare forhold efter artikel 10.

2. Bekendtgørelser om passende og specifikke foranstaltninger ved behandling af følsomme personoplysninger

Aalborg Kommune forstår lovforslagets § 3, stk. 2, således, at bestemmelsen ikke etablerer selve retsgrundlaget for behandling af følsomme personoplysninger, men giver ressortministrene mulighed for at fastsætte yderligere passende og specifikke foranstaltninger til beskyttelse af de registreredes rettigheder og interesser på deres respektive områder.

Kommunen noterer samtidig, at lovforslaget ikke indeholder en generel pligt til at udstede sådanne bekendtgørelser. Efter bemærkningerne skal behovet vurderes konkret, og der kan være tilfælde, hvor eksisterende sektorlovgivning eller allerede etablerede organisatoriske og tekniske foranstaltninger udgør tilstrækkelige garantier.

I dialogen med andre kommuner har der været tvivl om, hvorvidt lovforslagets § 3, st. 2 skal fortolkes som en bemyndigelse for ressortministrenes til at udstede bekendtgørelser om enten:

- Udelukkende fastsættelse af passende og specifikke foranstaltninger når der behandles følsomme personoplysninger, fordi det supplerende retsgrundlag allerede er givet i § 3, stk. 1 eller
- Særskilte supplerende retsgrundlag samt fastsættelse af passende og specifikke foranstaltninger som forudsætning for, at dette særskilte supplerende retsgrundlag på de enkelte områder finder anvendelse.

Forskellen består i, om offentlige myndigheder kan forvente, at de har det supplerende retsgrundlag til behandling af følsomme personoplysninger ved lovens ikrafttræden, eller om dette er afhængigt af udstedelse af konkrete bekendtgørelser på de enkelte områder.

Uanset hvilken fortolkning af lovforslagets § 3, stk. 2, der skal anlægges, anbefaler Aalborg Kommune i øvrigt, at der udvikles en så ensartet model som muligt for eventuelle bekendtgørelser efter § 3, stk. 2, således at krav og garantier bliver sammenhængende på tværs af sektorer og ressortområder. Det vil understøtte en mere ensartet implementering af loven og reducere risikoen for retlig usikkerhed.

3. Vejledning til afgrænsningen mellem beslutningsstøtte og øvrige AI-anvendelser

Aalborg Kommune anerkender Digitaliseringsstyrelsen for at udforme en legaldefinition af begrebet beslutningsstøtte.

Lovforslaget angiver hermed, at funktioner som referatskrivning, mødeindkaldelser, tale-til-tekst, simple chatbots og intelligente søgefunktioner falder uden for begrebet beslutningsstøtte, mens AI-systemer med væsentlig indflydelse på afgørelser eller væsentlige tiltag omfattes. Grænsen kan imidlertid være vanskelig at anvende på generative AI-værktøjer, som både kan anvendes som en simpel chatbot, men som også vil kunne anvendes til at give medarbejderen faglige anbefalinger, sammenfatninger eller vurderinger.

Aalborg Kommune skal derfor anmode om en vejledning med flere eksempler på grænsen mellem indgribende behandlinger og ikke-indgribende behandlinger, kriterier for vurderingen af, hvornår et output har væsentlig indflydelse på en afgørelse eller et tiltag, og vejledning om klassifikation af generative AI-værktøjer, der kan anvendes til behandlinger, der formentlig både er og ikke er beslutningsstøtte. I denne forbindelse anmoder Aalborg Kommune om en nærmere beskrivelse af, hvilken betydning behandling af følsomme personoplysninger tillægges ved vurderingen af, om en AI-anvendelse må anses for indgribende. Det fremstår ikke klart, om behandlingen af følsomme personoplysninger i sig selv taler for, at der skal stilles skærpede krav til retsgrundlaget, eller om dette alene er ét element blandt flere i den samlede vurdering af behandlingens karakter og konsekvenser.

4. Krav til reel menneskelig kontrol

Aalborg Kommune er enig i, at beslutningsstøtte forudsætter en reel og selvstændig menneskelig vurdering, og at kontrollen ikke må være en formalitet. Lovforslaget præciserer dog ikke i tilstrækkelig grad de operationelle krav til den menneskelige kontrol.

Aalborg Kommune skal derfor anmode om, at det behandles i en vejledning hvilke kompetencer den ansvarlige medarbejder skal have, hvilken indsigt medarbejderen skal have i systemets væsentligste forudsætninger, begrænsninger og usikkerheder, hvordan medarbejderens reelle mulighed for at ændre eller tilsidesætte output skal sikres, og hvordan den menneskelige kontrol skal dokumenteres i den enkelte sag og på overordnet niveau for selve systemet.

5. Beslutningsstøtte som behandlingsaktivitet

Lovforslaget omtaler flere steder beslutningsstøtte som en behandlingsaktivitet. Det adskiller sig fra den tilgang, der normalt anvendes i kommunale fortegnelser, hvor behandlingsaktiviteter typisk afgrænses efter opgaver, arbejdsgange eller processer. Beslutningsstøtte bør derimod beskrive en funktion i et bestemt led i en arbejdsgang, som kan indgå i flere forskellige behandlingsaktiviteter.

Aalborg Kommune skal derfor anmode om, at det i det endelige lovforslag, der fremsættes for Folketinget, præciseres om beslutningsstøtte skal registreres som en selvstændig behandlingsaktivitet, eller om beslutningsstøtte skal beskrives som et understøttelsesværktøj af den eksisterende opgave eller arbejdsgang.

6. Datadeling og fællesoffentlige AI-løsninger

Lovforslaget giver mulighed for viderebehandling af oplysninger inden for den enkelte myndighed, men etablerer ikke en generel hjemmel til videregivelse mellem myndigheder med henblik på udvikling eller anvendelse af AI-systemer. Afgrænsningen kan uhensigtsmæssigt vanskeliggøre udvikling af fælleskommunale og fællesoffentlige AI-løsninger, da disse ofte forbedres ved netop at samkøre eller træne løsninger på flere myndigheders enslignende data. Aalborg Kommune skal derfor anmode om, at det i det endelige lovforslag, der fremsættes for Folketinget, adresseres, om det er hensigten med lovforslaget at hindre samarbejde på tværs af offentlige myndigheder, når

myndighedernes data, herunder personoplysninger, kunne anvendes til fælles træning af AI-algoritmer eller lignende.

Hvis ovenstående begrænsning er hensigten med den foreslåede ordning, ønskes det adresseret hvordan myndigheder forventes at kunne udvikle og afprøve fælles AI-løsninger, når de relevante trænings- eller testdata befinder sig hos flere myndigheder.

7. Registreredes rettigheder

Lovforslagets § 4 giver mulighed for ved bekendtgørelse at begrænse rettigheder efter databeskyttelsesforordningens artikel 12 og 15-21, når betingelserne i artikel 23 er opfyldt. Aalborg Kommune noterer, at anvendelsesområdet er snævert, og at generelle ressource- eller effektiviseringshensyn ikke i sig selv kan begrunde en begrænsning.

Aalborg Kommune skal derfor anmode om, at det i bemærkningerne til det endelige lovforslag, der fremsættes for Folketinget, adresseres i hvilke konkrete situationer bemyndigelsen forventes anvendt, og hvilke typer AI-systemer eller behandlingssituationer der efter styrelsens vurdering kan opfylde nødvendigheds- og proportionalitetskravet for tilsidesættelse af de registreredes rettigheder.

8. Forvaltningsretlige krav og dokumentation

Aalborg Kommune er enig i lovforslagets bemærkninger om, at lovforslaget ikke kan ændre på de almindelige forvaltningsretlige regler og principper.

Det er imidlertid ikke nærmere beskrevet, hvordan myndighederne i praksis skal sikre og dokumentere notatpligt, partsindsigt, aktindsigt, korrekt sagsoplysning og begrundelse, når et AI-system bidrager til sagsbehandlingen.

Aalborg Kommune skal derfor anmode om en uddybende vejledning om hvilke oplysninger om systemets input, output og betydning for den konkrete sag, der skal journaliseres, og hvordan aktindsigts-, partsaktindsigts- og indsigtsrets-anmodninger håndteres, når relevante oplysninger eksempelvis kun findes i logs eller teknisk dokumentation.

Aalborg Kommune anbefaler, at Digitaliseringsstyrelsen i samarbejde med relevante myndigheder udarbejder en praktisk vejledning om de forvaltningsretlige dokumentationskrav ved anvendelse af AI.

Afsluttende bemærkninger

Aalborg Kommune støtter intentionen om at skabe et klarere retligt grundlag for en ansvarlig og værdiskabende anvendelse af AI i den offentlige sektor. For at loven kan få den tilsigtede praktiske virkning, er det afgørende, at de centrale snitflader til sektorlovgivningen, databeskyttelsesretten og forvaltningsretten omsættes til operationelle og ensartede krav.

Aalborg Kommune bidrager gerne til det videre arbejde med vejledningsmateriale, eksempler og eventuelle ressortspecifikke bekendtgørelser, navnlig hvor reglerne skal kunne anvendes på tværs af kommunale fagområder.

Venlig hilsen

Tommy Christiansen
Kommunaldirektør

Jan Nielsen
Direktør for Senior og Rehabilitering

Du kan altid kontakte Aalborg Kommune sikkert på www.aalborg.dk/kontakt eller via Digital Post på www.borger.dk.
Har du brug for hjælp til Digital Post, kan du ringe til Den Digitale Hotline på 7020 0000.
Læs om dine rettigheder og hvordan vi behandler personoplysninger på www.aalborg.dk/gdpr.

AARHUS KOMMUNE

12-10-2026

Til

Digitaliseringsstyrelsen jonmei@digst.dk

kopi til kahevi@digst.dk , emimol@digst.dk , leaomd@digst.dk

Høringssvar fra Magistratsafdelingen for Sundhed og Omsorg, Aarhus Kommune vedrørende Forslag til Lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger (AI-hjemmelsloven)

Magistratsafdelingen for Sundhed og Omsorg, Aarhus Kommune vil gerne bidrage med høringssvar til Digitaliseringsstyrelsens udkast til forslag til lov om offentlige myndigheders og organers udvikling og anvendelse af AI-systemer ved behandling af personoplysninger.

Generelle bemærkninger

Aarhus Kommune finder det overordnet meget positivt, at der med dette lovforslag søges at etablere et generelt hjemmelsgrundlag, som på tværs af ressortområder skal give offentlige myndigheder mulighed for at behandle personoplysninger til udvikling og anvendelse af AI.

Allerførst skal Aarhus Kommune imidlertid gøre Digitaliseringsstyrelsen opmærksom på, at Aarhus Kommune med den indledningsvise gennemgang fik dén forståelse, at lovforslaget alene ville etablere et generelt supplerende retsgrundlag for brug af almindelige personoplysninger til udvikling og anvendelse af AI, når disse personoplysninger i forvejen behandles som led i myndighedens opgavevaretagelse efter anden lovgivning.

I forhold til brug af følsomme personoplysninger var det Aarhus Kommunes umiddelbare forståelse, at det med lovforslaget stadig ville være uklart hvad der skal til, for at der er etableret de nødvendige passende foranstaltninger på et givent resort område.

Aarhus Kommune forstod ordlyden således, at lovforslaget lader det være op til den enkelte ressortminister at vurdere dette og - i forlængelse heraf - udstede de yderligere bekendtgørelser, der vurderes nødvendige.

Aarhus Kommunes analyse var herefter, at når en ressortminister således vil skulle vurdere om der er behov for en supplerende bekendtgørelse, for at det nødvendige retsgrundlag etableres, så kan ministeren kun tage udgangspunkt i de kriterier, der fremgår af hidtidig praksis og vejledninger fra Datatilsynet. Herefter ville resultatet nødvendigvis typisk lede til samme konklusion som i dag; nemlig at der vil være brug for supplerende bekendtgørelser i langt de fleste tilfælde.

Efter dialog med andre kommuner og KL, som oplyser at have holdt et møde med Digitaliseringsministeriet om lovudkastet, er det imidlertid blevet Aarhus Kommunes forståelse, at hensigten er, at lovudkastet *i sig selv* skal etablere og fungere som det supplerende retsgrundlag for behandling af både almindelige og følsomme personoplysninger, samt oplysninger om strafbare forhold.

Henset til ovenstående, samt til at Aarhus Kommune kan konstatere, at den beskrevne usikkerhed og misforståelse er / har været udbredt, er det af afgørende betydning for lovforslagets praktiske anvendelighed, at det af den endelige lovtekst og dennes bemærkninger fremgår eksplicit og utvetydig, hvilken af ovenstående tolkninger, der er den korrekte.

Bemærkninger til de enkelte dele af lovforslaget

§ 3, stk. 1

Når lovens anvendelsesområde begrænses til "AI-systemer", som defineret i AI forordningen, vil mange systemer ikke være omfattet.

Ved at udelukke simplere softwareløsninger fra lovforslagets anvendelsesområde, skabes et incitament til at udvikle og anvende AI-systemer til opgaver, som en simplere RPA-løsning måske ville have kunnet varetage.

Brug af AI, hvor opgaven kunne være løst ved hjælp af en mindre indgribende databehandling, vil alt andet lige medføre en mere kompleks og indgribende persondatabehandling end det simplere alternativ, hvilket ikke flugter med det databeskyttelsesretlige proportionalitetsprincip.

Det kunne overvejes at supplere med en formulering som ”*og lignende digitale løsninger.*”

§ 3, stk. 2

Bestemmelsen giver den enkelte minister mulighed for at udstede en supplerende bekendtgørelse, som fastsætter de beskyttelsesforanstaltninger, ministeren vurderer passende for eget område.

Eftersom det er lovforslagets hensigt i sig selv at udgøre det nødvendige supplerende retsgrundlag, og eftersom ministrene ikke pålægges en pligt, men alene en mulighed for dertil at udstede yderligere bekendtgørelser, må dette forventes at kunne give visse udfordringer i forhold til bestemmelsens praktiske anvendelighed:

For det første kan ordningen medføre usikkerhed om hvorvidt der vil komme en bekendtgørelse på et givent område, hvilket kan føre til forsinkelser eller unødig overforsigtighed i AI-projekter grundet usikkerhed om § 3, stk. 2 er ”nok”.

For det andet består den risiko, at der udstedes bekendtgørelser, som indeholder forskellige og indbydes uforenelige krav og beskyttelsesniveauer på tværs af ressortområder, som i den ”virkelige verden” sameksisterer i et uadskilleligt overlap.

Det gælder f.eks. på ældre- og omsorgsområdet, hvor regler fra servicelov, ældrelov og sundhedslov ofte flyder sammen i den praktiske ældrepleje.

For det tredje kan man forstille sig et scenarie, hvor socialministeren har udstedt en bekendtgørelse vedr. serviceloven, men hvor ældreministeren ikke har udstedt en bekendtgørelse vedr. ældreloven, og hvor reglernes asymmetri herefter gør det vanskeligt eller umuligt at udvikle og anvende AI, som skal benyttes i en arbejdsgang, hvori der opereres under begge regelsæt på samme tid.

På den baggrund er det Aarhus Kommunes anbefaling, at der i lovforslagets bemærkninger opstilles tydeligere kriterier for og eksempler på hvornår der skal udarbejdes yderligere bekendtgørelser.

Derudover kan overvejes en løsning, hvor alle ressortministerier, hvis lovgivninger er i spil i den praktisk-operationelle del af ældreplejen, i en koordineret indsats enten

1) udarbejder en samlelov, der etablerer det nødvendige, supplerende retsgrundlag i én og samme bekendtgørelse, eller
2) udarbejder eventuelle bekendtgørelser, der er enslydende og operationelt meningsgivende i forhold til hinanden og den praktiske virkelighed, de finder anvendelse i.

Begrebet "indgribende behandling"

Det fremgår af lovforslagets bemærkninger, at lovforslaget har til formål at skabe et generelt nationalt retsgrundlag for behandlingsaktiviteter, der ved brug af AI-systemer, må anses for at være indgribende.

I den forbindelse eksemplificerer lovforslaget, at ikke-indgribende behandlingsaktiviteter fx kan være AI-systemer, der anvendes til mødeindkaldelser, tale-til-tekst eller referatskrivning, *i det omfang*, der er tale om almindelige oplysninger.

Det fremgår imidlertid ikke hvilken betydning behandling af følsomme personoplysninger skal tillægges ved vurderingen af, om én af de ovenfor nævnte AI-systemer (stadig) skal anses for ikke-indgribende.

På den baggrund anbefales det, at der i bemærkningerne tilføjes en beskrivelse af hvorvidt eller under hvilke omstændigheder ovenstående eksempler på AI-systemer skal betragtes som indgribende, når der behandles følsomme oplysninger i disse systemer.

Menneskelig involvering

Lovforslaget angiver, at beslutningsstøtte forudsætter en reel menneskelig kontrol. Det er Aarhus Kommune enig i. Lovforslaget angiver desuden, at menneskelig involvering i så ringe en grad, at det må anses som en formalitet, ikke vil kunne anses som beslutningsstøtte. Det anbefales, at lovforslaget i den forbindelse tilføjes eksempler på en menneskelig involvering, der udgør den tilstrækkelige, reelle stillingtagen til AI-systemets forslag.

AARHUS KOMMUNE

12-10-2026

Yderligere sparring

Magistratsafdelingen for Sundhed og Omsorg, Aarhus Kommune står meget gerne til rådighed for yderligere bidrag og sparring, hvis det vurderes værdifuldt for jer.

Med venlig hilsen

Signe Rønn Sørensen, Forvaltningschef og

Pernille Jespersen, Juridisk specialkonsulent, Databeskyttelse