DATATILSYNET

3. marts 2026

J.nr. 2026-11-0479
Dok.nr. 840361
Sagsbehandler

Høring over udkast til forslag til lov om udvikling og anvendelse af AI-systemer ved behandling af personoplysninger i den offentlige forvaltning

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Digitaliseringsstyrelsen har den 12. februar 2026 anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte udkast til lovforslag.

Datatilsynet skal i den forbindelse udtale følgende:

1. Generelle bemærkninger

1.1. Datatilsynet skal generelt bemærke, at databeskyttelsesreglerne er teknologineutrale. Behandling af personoplysninger skal ske i overensstemmelse med reglerne, uanset om oplysningerne behandles ved brug af kunstig intelligens ("AI") eller ved brug af mere traditionelle it-værktøjer og systemer. Udvikling og anvendelse af AI kan indebære en yderligere og mere indgribende behandling af personoplysninger med deraf følgende risici for borgerne, som de dataansvarlige myndigheder skal kunne identificere og håndtere.

1.2. Det fremgår bl.a. af afsnit 1.1. i udkastets almindelige bemærkninger, at formålet med lovforslaget er at skabe en generel databeskyttelsesretlig hjemmel.

Herefter fremgår det, at en generel databeskyttelsesretlig hjemmel vil indebære, at myndigheder i den offentlige forvaltning – som led i myndighedens allerede fastlagte og afgrænsede opgavevaretagelse – vil kunne beslutte at behandle personoplysninger ved brug af kunstig intelligens i form af et AI-system til bl.a. beslutningsstøtte, herunder til evaluering af bestemte personlige forhold vedrørende en borger.

Det fremgår derudover, at lovforslaget helt overordnet vil gøre det muligt for myndigheder i den offentlige forvaltning at anvende AI-systemer på samme måde, som myndigheder i dag anvender andre elektroniske hjælpemidler til deres sagsbehandling.

Datatilsynet skal indskærpe, at en given hjemmel til behandling af personoplysninger ikke i sig selv sikrer, at de behandlingsaktiviteter, som foretages i forbindelse med udvikling og anvendelse af AI, sker lovligt.

Den dataansvarlige myndighed skal, inden en behandling af personoplysninger påbegyndes, stadig have overblik over og kunne dokumentere, at hele databeskyttelsesforordningen[1], databeskyttelsesloven[2] og anden for behandlingerne relevant lovgivning kan overholdes.

Datatilsynet har i flere sammenhænge udtalt, at man som dataansvarlig ikke lovligt kan benytte produkter, hvor aftalegrundlaget eller behandlingerne, der foretages, indebærer uklare behandlingskonstruktioner. Dette gør sig også gældende for det anvendelsesområde, udkastet vedrører.

Endvidere har Datatilsynet indskærpet, at den dataansvarlige skal have adgang til de nødvendige ressourcer til at sikre lovlig behandling af personoplysninger.[3] Det gælder også i situationer, hvor et valgt produkt eller aftalegrundlaget for produktet ændrer sig, hvilket efter tilsynets opfattelse ofte gør sig gældende på udkastets anvendelsesområde.

Datatilsynet bemærker, at der for de behandlingsaktiviteter, udkastet vedrører, skal være fokus på de grundlæggende databeskyttelsesretlige principper i databeskyttelsesforordningen. Særligt princippet om gennemsigtighed og kravet om rimelighed set i forhold til den registrerede, jf. artikel 5, stk. 1, litra a, princippet om dataminimering, jf. artikel 5, stk. 1, litra c, og kravet om at personoplysningerne skal være korrekte og om nødvendigt ajourførte, jf. artikel 5, stk. 1, litra d, er forhold, der ofte er centrale i forhold til udvikling og anvendelse af AI-systemer. Inden en behandling af personoplysninger påbegyndes skal den dataansvarlige myndighed kunne påvise, at de grundlæggende principper er overholdt, jf. databeskyttelsesforordningens artikel 5, stk. 2.

Alle de grundlæggende princippers effektive implementering skal – i det omfang databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design tilsiger det – gennemføres ved passende tekniske og organisatoriske foranstaltninger i AI-systemet. Endvidere skal AI-systemet indrettes på en måde, som muliggør, at principperne efterleves i hele AI-systemets livscyklus.

Den dataansvarliges forståelse af AI-systemets opbygning og de behandlinger, der foretages, er også nødvendig for at kunne sikre, at de registrerede kan udøve deres rettigheder i medfør af databeskyttelsesforordningens kapitel 3.

Det er efter Datatilsynets opfattelse helt grundlæggende en forudsætning for udvikling af solide, langtidsholdbare AI-systemer i den offentlige sektor og for en demokratisk og hensigtsmæssig teknologisk udvikling af samfundet, at udnyttelsen af potentialet i personoplysningerne sker med respekt for borgernes grundlæggende rettigheder. Det er det, databeskyttelsesreglerne skal sikre[4].

Herudover bemærker Datatilsynet, at der ved myndigheders 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 det er hensigten, at systemet skal vide-

1 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 (generel forordning om databeskyttelse).
2 Lovbekendtgørelse nr. 289 af 8. marts 2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
3 Der henvises til Datatilsynets afgørelse i sagen med j.nr. 2025-431-0053 (den såkaldte Chromebook-sag).
4 Se også regeringens strategiske indsats for kunstig intelligens fra december 2024, herunder navnlig afsnittet med overskriften "En ansvarlig ramme for kunstig intelligens i Danmark", side 20 ff., hvor det bl.a. er anført. at det er nødvendigt at sætte hegnspæle op og sikre en fælles juridisk ramme for brugen af kunstig intelligens, så teknologien ikke misbruges til eksempelvis at krænke vores grundlæggende rettigheder, vores privatliv og ytringsfrihed.

reudvikles ved brug af personoplysninger om borgerne, som den pågældende myndighed er dataansvarlig for.

Det skyldes, at AI-systemer ofte er karakteriseret ved betydelig kompleksitet og manglende gennemsigtighed. Det kan derfor 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 de registrerede – 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.

1.3. Det fremgår af afsnit 1 i udkastets almindelige bemærkninger, at Digitaliseringsministeriet vurderer, at der generelt kan være en række potentialer forbundet med myndighedernes 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 ifølge ministeriet både i forbindelse med sagsbehandling og i opgavevaretagelsen i sin helhed – både i forhold til anvendte ressourcer og i løftet af kvaliteten i disse opgaver.

Datatilsynet ser gerne, at det nuanceres i udkastets bemærkninger, at der udover de ressourcebetragtninger, Digitaliseringsministeriet henviser til, skal påregnes et ikke ubetydeligt arbejde med at sikre overholdelsen af de databeskyttelsesretlige regler, som følge af de problemstillinger, der er nævnt ovenfor i afsnit 1.2. Et arbejde, der skal foretages inden behandlingerne påbegyndes[5], men som nævnt ovenfor naturligvis også løbende i 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. Anvendelsesområde

2.1. Udkastets § 1 vedrører lovens anvendelsesområde. Det fremgår af afsnit 2.1.2. i udkastets almindelige bemærkninger, at det er Digitaliseringsministeriets vurdering, at det vil være afgørende, at den foreslåede ordning finder anvendelse på hele den offentlige forvaltning.

Lovens anvendelsesområde er organisatorisk afgrænset. Det afgørende for, om en organisations behandlingsaktiviteter er omfattet af lovens anvendelsesområde, er, om organisationen er omfattet af forvaltningslovens § 1, stk. 1-3.

Det fremgår af udkastets § 1, stk.1, at loven gælder for alle dele af den offentlige forvaltning, jf. forvaltningslovens § 1, stk. 1.

Endvidere fremgår det af udkastets § 1, stk. 2, at i overensstemmelse med forvaltningslovens § 1, stk. 2, gælder loven desuden for al virksomhed, der udøves af 1) selvejende institutioner, foreninger, fonde m.v., der er oprettet ved lov eller i henhold til lov, og selvejende institutioner, foreninger, fonde, m.v., der er oprettet på privatretligt grundlag, og som udøver offentlig virk-

5 Se Datatilsynets vejledning og skabelon til en konsekvensanalyse i forhold til AI-systemer, jf. databeskyttelsesforordningens artikel 35.

somhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentligt tilsyn og intensiv offentlig kontrol.

Det fremgår herudover af udkastets § 1, stk. 3, at loven gælder for nærmere angivne selskaber, institutioner, foreninger m.v., efter anden lovgivning og regler i overensstemmelse med forvaltningslovens § 1, stk. 3.

Ifølge udkastets bemærkninger til § 1, stk. 3, vil den foreslåede bestemmelse medføre, at loven vil gælde for nærmere angivne selskaber, institutioner, foreninger m.v., hvis udgifterne ved deres virksomhed overvejende dækkes af statslige, regionale eller kommunale midler, eller i det omfang de ved eller i henhold til lov har fået tillagt beføjelse til at træffe afgørelser på det offentliges vegne. Det fremgår endvidere, at den foreslåede bestemmelse vil sikre, at lovforslaget tillige vil dække virksomheder og institutioner, der overvejende dækkes af statslige, regionale eller kommunale midler, herunder direkte tilskud, medlemsbidrag eller egentlige betalinger for modydelser.

Datatilsynet forstår det på den baggrund sådan, at det er hensigten, at loven også skal finde anvendelse på nogle af de behandlingsaktiviteter, der ikke er omfattet af databeskyttelsesforordningens og databeskyttelseslovens anvendelsesområde. Der henvises i den forbindelse til databeskyttelsesforordningens artikel 2, stk. 2, og databeskyttelseslovens § 3, jf. også nedenfor.

2.2. Datatilsynet forstår det endvidere sådan, at det er hensigten, at loven også skal finde anvendelse på retshåndhævende myndigheders, herunder politiets, behandling af personoplysninger, som foretages med henblik på varetagelsen af opgaver knyttet til det strafferetslige område. Dette fremgår dog ikke klart af bemærkningerne i udkastet.

Databeskyttelsesforordningen og databeskyttelsesloven gælder ikke for behandling af personoplysninger, der foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed. Det følger af databeskyttelsesforordningens artikel 2, stk. 2, litra d.

Derimod gælder retshåndhævelsesloven[6] for politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, Danmarks Fængsler, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger på dette område. Det følger af retshåndhævelseslovens § 1, stk. 1.

I udkastets bemærkninger er det primært databeskyttelsesforordningen og databeskyttelsesloven, der er omtalt. Om retshåndhævelsesloven fremgår dog følgende af afsnit 2.1.1.1. i udkastets almindelige bemærkninger:

> ”Endelig skal det bemærkes, at der på visse områder og sektorer findes anden lovgivning, som regulerer behandlingen af personoplysninger udover reglerne i databeskyttelsesforordningen og databeskyttelsesloven. Dette omfatter bl.a. retshåndhævelsesdirektivet (Europa-Parlamentets og Rådets direktiv 2016/680/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA), som er gennemført i dansk ret ved lov nr. 410 af 27. april 2017 om

6 Lov nr. 410 af 27. april 2017 med senere ændringer om retshåndhævende myndigheders behandling af personoplysninger med senere ændringer.

> retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven). Den foreslåede ordning vil ikke kunne finde anvendelse i strid med sådan særlovgivning."

Datatilsynet bemærker i den forbindelse, at retshåndhævelsesloven ikke regulerer behandlingen af personoplysninger udover reglerne i databeskyttelsesforordningen og databeskyttelsesloven. Det er derimod regler, der finder anvendelse på behandlingen af personoplysninger på et område, hvor databeskyttelsesforordningen og databeskyttelsesloven ikke gælder.

Det bør efter Datatilsynets opfattelse tydeliggøres, at udkastet også gælder for den behandling af personoplysninger, der er omfattet af retshåndhævelsesloven. Herudover bør Digitaliseringsministeriet forholde sig til de særlige regler, der gælder for denne behandling af personoplysninger i lovudkastets bemærkninger.

2.3. Det står endvidere ikke Datatilsynet klart, om det er hensigten, at reglerne i udkastet også skal gælde for politiets og forsvarets efterretningstjenesters behandling af personoplysninger.

Det følger af databeskyttelseslovens § 3, stk. 2, at databeskyttelsesloven og databeskyttelsesforordningen ikke finder anvendelse på den behandling af personoplysninger, som udføres for eller af politiets og forsvarets efterretningstjenester.

Politiets Efterretningstjenestes behandling af personoplysninger er reguleret af lov om Politiets Efterretningstjeneste og bekendtgørelse om Politiets Efterretningstjenestes behandling af oplysninger om fysiske og juridiske personer m.v.[7], og Forsvarets Efterretningstjenestes behandling af personoplysninger er reguleret af lov om Forsvarets Efterretningstjeneste og bekendtgørelse om behandlingssikkerhed ved Forsvarets Efterretningstjenestes behandling af personoplysninger.[8]

Det bør efter Datatilsynets opfattelse præciseres, om udkastet også gælder for den behandling af personoplysninger, som udføres for eller af politiets og forsvarets efterretningstjenester. Herudover bør Digitaliseringsministeriet i givet fald forholde sig til de særlige regler, der gælder for denne behandling af personoplysninger i lovforslagets bemærkninger.

3. Definitioner

"Beslutningsstøtte" defineres i udkastets § 2, nr. 4 som: "Enhver form for forslag eller anbefaling til afgørelser eller 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."

Datatilsynet har noteret sig, at forslag eller anbefalinger til tiltag også er omfattet af definitionen. Datatilsynet lægger derfor til grund, at det også vil omfatte faktisk forvaltningsvirksomhed.

Det fremgår af afsnit 2.1.2. i udkastets almindelige bemærkninger, at den foreslåede ordning ikke vil give hjemmel til at træffe automatiske afgørelser, dvs. afgørelser uden menneskelig involvering. Datatilsynet ser gerne, at der henvises til databeskyttelsesforordningens ordlyd i artikel 22, også set i forhold til profilering, som er defineret forordningens artikel 4, nr. 4.

I den forbindelse fremgår i øvrigt følgende af det nævnte afsnit:

7 Lovbekendtgørelse nr. 231 af 07. marts 2017 om Politiets Efterretningstjeneste (PET) med senere ændringer og bekendtgørelse nr. 763 af 20. juni 2014 om Politiets Efterretningstjenestes behandling af oplysninger om fysiske og juridiske personer m.v.
8 Lovbekendtgørelse nr. 1287 af 28. november 2017 om Forsvarets Efterretningstjeneste (FE) med senere ændringer og bekendtgørelse nr. 1028 af 11. juli 2018 om behandlingssikkerhed ved Forsvarets Efterretningstjenestes behandling af personoplysninger

> ”I forhold til kravet om, hvor stor den menneskelige involvering skal være, førend der er tale om beslutningsstøtte og ikke automatisk sagsbehandling, er ikke fastlagt klart i retspraksis. Det må derfor forventes, at fremtidig retspraksis 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 automatisk sagsbehandling, f.eks. efter databeskyttelsesforordningens artikel 22 om automatiske individuelle afgørelser, herunder profilering.”

Datatilsynet bemærker, at også tilsynets praksis, herunder praksis fra Det Europæiske Databeskyttelsesråd (EDPB), om databeskyttelsesforordningens artikel 22 vil bidrage til at præcisere dette.

Derudover bemærker Datatilsynet, at en særlig risiko, som der bør være opmærksomhed på er ”automation bias”. Denne risiko er også omtalt i afsnit 4 i udkastets almindelige bemærkninger om ligestillingsmæssige konsekvenser. Det er tilfælde, hvor f.eks. sagsbehandlere tillægger systemets vurdering af en sag større betydning end deres egen vurdering, hvilket fører til, at systemet derfor de facto afgør sagen.

Artikel 29-gruppen har udtalt i sine retningslinjer om automatiske individuelle afgørelser og profilering, at for at det kan betragtes som menneskelig indgriben skal den dataansvarlige sikre, at et tilsyn med afgørelsen er meningsfuldt og ikke blot en tom gestus. Det bør i øvrigt foretages af en person, der har den fornødne kompetence og mulighed for at ændre afgørelsen. [9]

Det må for at sikre denne meningsfuldhed tilsvarende gælde, at de personer, der reelt skal træffe afgørelsen, sættes i stand til at evaluere på de faktuelle omstændigheder, der præsenteres, sådan at det til enhver tid kan verificeres, at det nødvendige og retvisende faktum inddrages i sagens afgørelse.

Derudover fremgår det af Artikel 29-gruppens retningslinjer, at den dataansvarlige som led i konsekvensanalysen vedrørende databeskyttelse bør identificere og registrere omfanget af enhver menneskelig indgriben i beslutningsprocessen, og hvornår i processen en sådan indgriben skal ske.

4. Supplerende retsgrundlag

4.1. Det følger af udkastets § 3, stk. 1, at myndigheder inden for den offentlige forvaltning kan udvikle og anvende AI-systemer, herunder gøre brug af beslutningsstøtte, på baggrund af personoplysninger, myndigheden behandler, for at understøtte myndighedens opgavevaretagelse efter anden lovgivning.

Derudover følger af udkastets § 3, stk. 2, at vedkommende minister på eget ressort skal fastsætte 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 og artikel 10, og sådanne foranstaltninger er påkrævet i henhold til databeskyttelsesreglerne.

Datatilsynet har forstået, at det er hensigten, at § 3, stk. 1, skal fungere som supplerende retsgrundlag for behandling af personoplysninger i forbindelse med udvikling og anvendelse af AI-systemer i alle sammenhænge og på alle områder i den offentlige forvaltning.

9 Side 21-22 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. Der henvises i øvrigt til afsnit 3.6.2. i Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens.

Det er i den forbindelse Datatilsynets forståelse, at de særlige kategorier af oplysninger, der er omfattet af databeskyttelsesforordningens artikel 9, stk. 1, og artikel 10 alene kan behandles i den forbindelse, efter at ressortministerierne ved bekendtgørelse har fastsat yderligere foranstaltninger for beskyttelse af den registreredes rettigheder og frihedsrettigheder, hvis det vurderes at være nødvendigt efter databeskyttelsesreglerne. I den forbindelse skal ressortministerierne vurdere, om det efter databeskyttelsesreglerne er nødvendigt at fastsætte yderligere foranstaltninger.

Det følger af databeskyttelsesforordningens artikel 6, stk. 1, litra e, at behandlingen af personoplysninger er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

Behandling af personoplysninger på baggrund af databeskyttelsesforordningens artikel 6, stk. 1, litra e, kræver, at der foreligger et såkaldt supplerende retsgrundlag, som forpligter eller berettiger myndigheden til at udføre en bestemt myndighedsopgave. Det følger af forordningens artikel 6, stk. 2 og 3.

Behandlingen af de særlige kategorier af oplysninger, der er oplistet i databeskyttelsesforordningens artikel 9, stk.1, er som udgangspunkt forbudt. Det skyldes, at behandlingen af disse typer oplysninger er forbundet med en særlig høj risiko for borgeren. Der kan kun ske undtagelse fra dette forbud i de tilfælde, som fremgår af artikel 9, stk. 2.

Som det også fremgår af afsnit 2.2.1.1.2. i udkastets almindelige bemærkninger, kræver behandlingen af de særlige kategorier af personoplysninger derudover, at der kan identificeres et lovligt behandlingsgrundlag efter artikel 6.

I afsnit 2.2.2.2 i udkastets almindelige bemærkninger er databeskyttelsesforordningens artikel 9, stk. 2, litra g, nævnt. Det følger af denne bestemmelse, at forbuddet efter artikel 9, stk. 1, ikke finder anvendelse, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

En fravigelse af forbuddet 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.

For så vidt angår oplysninger om strafbare forhold, der er omfattet af databeskyttelsesforordningens artikel 10 må oplysningerne ikke behandles af offentlige myndigheder, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver. Det følger af databeskyttelseslovens § 8, stk. 1.

I det omfang der er hjemmel til behandling af oplysninger om strafbare forhold i anden lovgivning, herunder den foreslåede § 3 i udkastet, skal der ikke derudover være hjemmel i databeskyttelseslovens § 8. Datatilsynet henviser i den forbindelse 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.

Digitaliseringsministeriet ses dog ikke i udkastets bemærkninger at have forholdt sig til databeskyttelsesforordningens artikel 10 i forhold til, om udkastets § 3 skal udgøre hjemmel til behandling af oplysninger om strafbare forhold.

4.2. Datatilsynet har i flere sammenhænge tidligere udtalt sig om kravene til supplerende retsgrundlag i forbindelse med offentlige myndigheders behandling af personoplysninger i forbindelse med udvikling og anvendelse af AI-systemer.[10]

For det første skal grundlaget for behandlingen fremgå af EU-retten eller national ret, jf. artikel 6, stk. 3, 1. pkt. Det skal således fremgå af lovregler, bekendtgørelser eller andre administrative forskrifter, at en myndighed er forpligtet eller berettiget til at udføre en bestemt myndighedsopgave. Der kræves ikke nødvendigvis en specifik lov for hver behandlingsaktivitet. Det kan være tilstrækkeligt med én lov som grundlag for flere behandlingsaktiviteter, som er nødvendige for at udføre en opgave i samfundets interesse eller som en del af offentlig myndighedsudøvelse.[11]

Retsgrundlaget skal for det andet være klart og præcist, og anvendelsen af reglerne bør være forudsigelig for de borgere, der omfattes af reglerne.[12]

Behandlingen af personoplysninger skal derudover være nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.[13]

Endelig er der et krav om, at medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, som forfølges. Databeskyttelsesforordningen fastsætter således et krav om proportionalitet og iagttagelse af samfundets interesse i forbindelse med national ret og EU-ret, der tilpasser anvendelsen af databeskyttelsesforordningen.[14]

Kravet til klarheden af det pågældende supplerende retsgrundlag afhænger generelt af, hvor indgribende behandlingen af personoplysninger vil være for borgeren. I vurderingen af, om retsgrundlaget er tilstrækkelig klart, bør det indgå, hvilke oplysninger der behandles og om hvilke personer, herunder f.eks. sårbare borgere. Derudover skal det indgå i vurderingen, om det output – f.eks. forslag eller anbefaling til afgørelse eller tiltag overfor en borger – som AI-systemet genererer, har indvirkning på borgerens økonomiske, uddannelsesmæssige, sociale, sundhedsmæssige eller lignende forhold. Indvirkningen kan være såvel positiv som negativ.

4.3. Generelt har Datatilsynet tidligere udtalt sig positivt om offentlige myndigheders brug af personoplysninger til at designe, udvikle og teste AI-systemer, som kan understøtte myndigheden i at varetage deres opgave, som de er forpligtet eller berettiget til at foretage efter anden lovgivning. Det skyldes, at udvikling af et AI-system som altovervejende udgangspunkt ikke medfører direkte konsekvenser for borgerne i form af f.eks. en afgørelse.

Behandlingen af oplysningerne i forbindelse med udvikling af et AI-system ligger ikke altid inden for borgernes rimelige forventninger til, hvad myndighederne vil bruge deres oplysninger

10 Der henvises til afsnit 4.1 og 4.2 i Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens, Datatilsynets udtalelse til Københavns Kommune i sagen med j.nr. 2023-212-0015, Datatilsynets udtalelser til Uddannelses- og Forskningsstyrelsen i sagen med j.nr. 2024-212-0371 og Datatilsynets udtalelse til Styrelsen for Arbejdsmarked og Rekruttering i sagen med j.nr. 2022-212-3676.
11 Præambelbetragtning nr. 45 til databeskyttelsesforordningen.
12 Præambelbetragtning nr. 41 til databeskyttelsesforordningen.
13 Databeskyttelsesforordningens artikel 6, stk. 3, 2. pkt
14 Databeskyttelsesforordningens artikel 6, stk. 3, sidste led.

til. Det kan derfor alt afhængig af omstændighederne være indgribende for en borger, at vedkommendes personoplysninger ikke alene anvendes i forbindelse med f.eks. en konkret sag, som vedkommende er involveret i, men at oplysningerne også anvendes til udvikling af et AI-system, der f.eks. skal sikre effektivitet og bedre kvalitet i sagsbehandlingen af den eller andre typer sager.

Et AI-system i drift vil forventeligt generere forudsigelser, anbefalinger mv., som f.eks. skal være beslutningsstøtte for myndighedens sagsbehandlere. Konsekvenserne for borgerne er dermed ofte større, når AI-systemet er i drift, og der stilles derfor højere krav til klarheden af det retsgrundlag, der danner baggrund for at anvende systemet i drift.

Det fremgår af udkastets bemærkninger til § 3, stk. 1, at myndigheder i den offentlige forvaltnings brug af AI-systemer til at varetage opgaver efter anden lovgivning bl.a. vil kunne omfatte beslutningsstøtte, herunder til evaluering af bestemte personlige forhold vedrørende en borger, men ikke er afgrænset hertil. Dette vil betyde, at beslutningsstøtte, herunder til evaluering af bestemte personlige forhold vedrørende en borger, vil kunne foretages, hvis det sker i forbindelse med myndighedens opgavevaretagelse.

Datatilsynet forstår det sådan, at det er hensigten, at det skal være muligt at foretage profilering[15] med AI-systemer, når de er i drift.

AI-systemer baseret på maskinlæring er særdeles effektive til profilering. Systemerne er ofte specifikt trænet til at finde bestemte mønstre i datasæt. Når systemet modtager inputdata, der vedrører en specifik borger, kan modellen generere den statistiske sandsynlighed for, at den pågældende borger f.eks. vil udvise en given adfærd eller udvikle en bestemt sygdom.

Datatilsynet har noteret sig, at det fremgår af afsnit 2.1.2. i udkastets almindelige bemærkninger, at den foreslåede ordning ikke vil give hjemmel til at træffe automatiske afgørelser, dvs. afgørelser uden menneskelig involvering.

I den forbindelse bemærker Datatilsynet, at dette ikke fremgår klart af ordlyden i § 3, stk. 1, hvor beslutningsstøtte nævnes som et af flere mulige formål med et AI-system, jf. brugen af ordet ”herunder”.

Endvidere bemærker Datatilsynet, at selv om der ikke med reglerne i udkastet vil være hjemmel til at træffe automatiske afgørelser uden menneskelig involvering, kan brugen af profilering til brug for beslutningsstøtte indebære, at anvendelsen af et AI-system er indgribende.

Dataansvarlige kan foretage profilering, hvis behandlingen opfylder alle de grundlæggende principper og har et retligt grundlag. Der er indført yderligere garantier og restriktioner i forbindelse med afgørelser, der alene er baseret på automatisk behandling, herunder profilering, som defineret i artikel 22, stk. 1. 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.[16]

15 Profilering er udtrykkeligt defineret i databeskyttelsesforordningens artikel 4, nr. 4 som ”enhver form for automatisk behandling med henblik på at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.
16 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.

Profilering kan indebære, at der behandles særlige kategorier af oplysninger, som kan udledes fra oplysninger, der ikke er særlige kategorier af oplysninger i sig selv, men som bliver det, når de kombineres med andre oplysninger.[17] Brugen af profilering medfører derudover nogle særlige forpligtelser i forhold til de registreredes rettigheder. De registrerede skal bl.a. informeres om tilstedeværelsen af profilering og konsekvensen heraf.[18]

Behandling af særlige kategorier af personoplysninger er forbundet med en særlig høj risiko for borgeren, og der stilles i sagens natur større krav til klarheden af det supplerende retsgrundlag, hvor disse typer oplysninger kan behandles. Datatilsynet har forstået, at dette er baggrunden for udkastets § 3, stk. 2.

Datatilsynet bemærker, at der kan være andre forhold, der medfører, at behandling af personoplysninger i forbindelse med anvendelse af et AI-system i drift er meget indgribende. Der kan f.eks. være tale om behandling af oplysninger om sårbare personer eller behandling af fortrolige oplysninger om f.eks. væsentlige sociale problemer eller andre rent private forhold, som ikke er omfattet af databeskyttelsesforordningens artikel 9 og 10. Derudover kan brugen af systemet have indvirkning på borgerens økonomiske, uddannelsesmæssige, sociale, sundhedsmæssige eller lignende forhold.

4.4. Datatilsynet anerkender de saglige formål, der ligger til grund for den generelle databeskyttelsesretlige hjemmel i udkastets § 3. Datatilsynet skal imidlertid pege på, at den foreslåede tilgang rejser væsentlige spørgsmål i relation til databeskyttelse.

Det skyldes, at udkastets bestemmelser 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 Datatilsynets opfattelse, at en så vid adgang som den foreslåede i udkastets § 3 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.

5. Anvendelse af data fra myndighedernes historiske og lukkede sager

Det fremgår af afsnit 2.2.2.1. i udkastets almindelige bemærkninger og bemærkningerne til udkastets § 3 bl.a., at det med udkastets § 3, stk. 1, vil være muligt at anvende data fra myndighedernes historiske og lukkede sager i forbindelse med udvikling af AI-systemer, hvor data vil kunne anvendes til at træne systemer i at identificere mønstre, der er relevante for systemets endelige opgave.

Derudover fremgår det af bemærkningerne til udkastets § 3, stk. 1, at bestemmelsen vil medføre, at myndigheder i den offentlige forvaltning kan behandle personoplysninger, som myndigheden har indsamlet til et formål, f.eks. konkret sagsbehandling, til et andet formål, navnlig

17 Side 16 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.
18 Præambelbetragtning nr. 60 til databeskyttelsesforordningen.

udvikling af et AI-system, uden at skulle foretage en nærmere vurdering af, om der er tale om forenelige formål. Dette skyldes, at der ifølge Digitaliseringsministeriet i henhold til databeskyttelsesforordningens artikel 6, stk. 4, vil være tale om viderebehandling på baggrund af national ret.

Det følger af databeskyttelsesforordningens artikel 6, stk. 4, at personoplysninger kan behandles til et andet formål end det, som oplysningerne er indsamlet til, uden at der skal foretages en vurdering af, om det nye formål ikke er uforeneligt med det oprindelige formål med indsamlingen af oplysningerne, hvis behandlingen er baseret på EU-retten eller medlemsstaternes nationale ret. Det er endvidere et krav, at medlemsstaternes nationale ret skal udgøre en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1.

Digitaliseringsministeriet ses ikke i udkastets bemærkninger 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 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 offentlige myndigheder samt de selskaber, institutioner, foreninger m.v., der er omfattet af forvaltningslovens § 1, stk. 2, og § 1, stk. 3, i alle sammenhænge kan viderebehandle oplysninger fra historiske og afsluttede sager til brug for udvikling af AI-systemer.

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.

Datatilsynet lægger til grund, at der ved en eventuel anvendelse af personoplysninger fra myndigheders historiske og lukkede sager er tale om sager, der endnu ikke er afleveret til et offentligt arkiv efter reglerne i arkivloven.[19]

Datatilsynet bemærker i den forbindelse, at de dataansvarlige myndigheder ved udvikling af AI-systemer skal tage højde for risikoen for unødvendig dataophobning.

Det følger af databeskyttelsesforordningens artikel 5, stk. 1, litra e, at personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. Personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder.

Princippet om opbevaringsbegrænsning indebærer, at en offentlig myndighed – på samme vis som alle andre dataansvarlige – generelt må sørge for, at behandling af personoplysninger bringes til ophør, når myndigheden har vurderet, at opbevaring m.v. ikke længere er nødvendig til de formål, hvortil oplysningerne er blevet behandlet. Myndigheden kan i den forbindelse

19 Bekendtgørelse nr. 1201 af 28. september 2016 af arkivloven med senere ændringer.

aflevere (dele af) oplysningerne til et offentligt arkiv, der har som hovedformål at bevare historisk værdifulde arkivalier og at stille arkivalierne til rådighed for borgere og myndigheder som dokumentation eller til almenkulturelle eller forskningsmæssige formål.[20]

Som følge af princippet om opbevaringsbegrænsning sammenholdt med arkivlovens regler om begrænset adgang til ikke umiddelbart tilgængelige arkivalier, er det Datatilsynets opfattelse, at når en offentlig myndighed 1) har vurderet, at oplysningerne ikke længere er nødvendige at behandle, 2) har afleveret oplysningerne til et offentligt arkiv og 3) herefter har slettet oplysningerne hos sig selv, skal oplysningerne som udgangspunkt anses for at være utilgængelige for både myndigheden selv og for andre myndigheder, der måtte have interesse i selv at indsamle og viderebehandle oplysningerne, der nu (kun) findes hos det offentlige arkiv.

Dette gælder efter Datatilsynets opfattelse, uanset at oplysningerne ved aflevering til et offentligt arkiv ikke de facto er slettet, og uanset at der er en vis adgang til at tilgå oplysningerne hos arkivet.

Når en myndighed har afleveret sine arkivalier til et offentligt arkiv, finder arkivlovens kapitel 6 om tilgængelighed til offentlige arkivalier anvendelse. Ifølge arkivlovens § 22, stk. 1, er arkivenheder, der er skabt eller tilvejebragt af den offentlige forvaltning og domstolene, og som er afleveret til offentligt arkiv, som udgangspunkt tilgængelige, når arkivenhederne er 20 år gamle. Ifølge § 23, stk. 1, er arkivenheder, som indeholder oplysninger om enkeltpersoners private, herunder økonomiske, forhold, dog først tilgængelige, når de er 75 år gamle.

Det følger af arkivlovens § 30, stk. 1, at enhver kan søge om tilladelse til benyttelse af ikke umiddelbart tilgængelige arkivalier, hvorved forstås arkivalier, hvor tilgængelighedsfristen ikke er udløbet. Adgang efter arkivlovens § 30 meddeles som dispensation fra de almindelige tilgængelighedsfrister. Det er bl.a. derfor Datatilsynets opfattelse, at der ikke kan forudsættes en vid adgang til at viderebehandle arkiverede oplysninger.

I det omfang arkivalierne er afleveret til Rigsarkivet, kan rigsarkivaren eller den, der af rigsarkivaren bemyndiges hertil, i henhold til arkivlovens § 31 meddele tilladelse i konkrete tilfælde til benyttelse af dokumenter, arkivenheder eller grupper af arkivenheder, som er afleveret til Rigsarkivet, inden udløbet af tilgængelighedsfristerne, jf. dog §§ 33-35.

Kommunalbestyrelserne eller regionsrådene kan i henhold til arkivlovens § 32 i konkrete tilfælde meddele tilladelse til benyttelse af dokumenter, arkivenheder eller grupper af arkivenheder, som er afleveret til et kommunalt eller regionalt arkiv, inden udløbet af tilgængelighedsfristerne, jf. dog § 34.

Det fremgår af arkivlovens § 34, at tilladelse efter §§ 31 og 32 kræver samtykke fra Datatilsynet, hvis arkivenheden er afleveret fra en myndighed inden for den offentlige forvaltning og indeholder oplysninger om enkeltpersoners rent private forhold *og* tidligere behandling af oplysningerne har været omfattet af persondataloven, databeskyttelsesforordningen, databeskyttelsesloven eller retshåndhævelsesloven eller oplysningerne stammer fra et edb-register, der har været ført for den offentlige forvaltning.

Datatilsynet har i en sag, der blev behandlet på et møde i Datarådet, meddelt Rigsarkivet, at tilsynet ikke kunne meddele samtykke til udlevering af det pågældende arkivmateriale til Gældsstyrelsen.[21]

20 Almindelige bemærkninger til lovforslag nr. 18 af 2. oktober 2002 til arkivlov.
21 Datatilsynets sag med j.nr. 2024-84-0272.

Gældsstyrelsen havde ansøgt Rigsarkivet om adgang til data fra arkivalier, der var blevet afleveret af andre myndigheder, og som styrelsen forventede vedrørte afgørelser eller aftaler om pligt til at betale underholdsbidrag samt opkrævning og inddrivelse af de krav på underholdsbidrag, der fremgår af afgørelsen eller aftalen. Gældsstyrelsen ønskede at benytte dataene fra Rigsarkivet til at teste og udvikle en database, der samtidig ville bestå af data fra styrelsen selv og andre myndigheder. Styrelsens endelige formål var at sagsbehandle konkrete inddrivelsessager vedrørende underholdsbidrag, hvor databasen skulle bruges til at undersøge og dokumentere, hvorvidt de enkelte krav fortsat var retskraftige, eller om de var forældede.

Datatilsynet oplyste Rigsarkivet i sagen, at det var tilsynets opfattelse, at der vil opstå risiko for, at offentlige myndigheders sletning af personoplysninger for at overholde databeskyttelsesforordningens artikel 5, stk. 1, litra e, reelt vil blive sat ud af kraft, hvis der blev givet mulighed for at få adgang til at foretage omfattende udtræk af andre myndigheders arkivmateriale med henblik på sagsbehandling, sådan som der var lagt op til i sagen.

I den pågældende sag lagde Datatilsynet bl.a. særlig vægt på, at der ønskedes adgang til en betragtelig mængde oplysninger, der skulle samkøres med andre datakilder med det endelige formål at foretage sagsbehandling vedrørende et større antal borgere.

Derudover bemærkede Datatilsynet i sagen, at det efter tilsynets opfattelse ikke kunne føre til en anden vurdering, at et afslag på samtykke kunne påføre Gældsstyrelsen et betydeligt ressourceforbrug med at indsamle de nødvendige oplysninger fra andre kilder, i det omfang det var muligt. Heller ikke den omstændighed, at det i visse tilfælde kunne medføre en økonomisk skade for myndigheden eller private borgere, kunne efter tilsynets opfattelse føre til en anden vurdering.

Det er Datatilsynets opfattelse, at mange af de bemærkninger, tilsynet anførte i den pågældende sag, vil dække behandling af de arkiverede personoplysninger på udkastets anvendelsesområde.

Datatilsynet gør i øvrigt opmærksom på, at behandling af oplysninger til andre formål end de oprindelige medfører, at borgerne skal oplyses om de(t) nye formål.

Denne pligt gælder dog ikke, hvis det udtrykkeligt fremgår af lovgivningen, at myndigheden foretager denne behandling af oplysningerne.

6. Undtagelse til de registreredes rettigheder

Det fremgår af udkastets § 4, 1. pkt., at vedkommende minister kan fastsætte regler om, at bestemmelserne i databeskyttelsesforordningens artikel 12 og artikel 15-21 ikke gælder, hvis ét af forholdene i databeskyttelsesforordningens artikel 23, stk. 1, gør sig gældende. Herefter fremgår det af bestemmelsen, 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 bl.a. af afsnit 1.1. i udkastets almindelige bemærkninger:

> ”Udover at danne retsgrundlag for behandling af personoplysninger til udvikling og anvendelse af AI-systemer, indeholder lovforslaget en mulighed for, at ressortministrene ved bekendtgørelse kan vælge at etablere undtagelser til en række af bestemmelserne i databeskyttelsesforordningen. Der vil således være mulighed for ressortministrene at gøre helt eller delvist undtagelse til en række af den registreredes rettigheder i databeskyttelsesforordningen under nærmere bestemte betingelser.

> Denne undtagelsesmulighed etableres i lovforslaget, da det er vurderet nødvendigt af hensyn til myndighederne i den offentlige forvaltning. Det skyldes særligt, at den tekniske opbygning af AI-systemer kan gøre det svært i alle tilfælde at tilgodese den registreredes rettigheder, f.eks. i forhold til retten til indsigt eller retten til sletning, jf. databeskyttelsesforordningens artikel 15 og 17."

Derudover fremgår bl.a. det følgende af afsnit 2.3.2.1. i udkastets almindelige bemærkninger:

> "Det er Digitaliseringsministeriets vurdering, at en mulighed for at gøre undtagelse eller lave begrænsning til den registreredes rettigheder er relevant i forbindelse med myndigheder i den offentlige forvaltnings udvikling og anvendelse af AI-systemer. AI-systemer er ofte kendetegnet ved komplekse datastrukturer, hvor oplysninger fra mange registrerede potentielt vil indgå i træningsdata, der ikke nødvendigvis tillader adskillelse af de individuelle data. Dermed kan AI-systemernes funktionsmåde gøre det vanskeligt, eller i visse tilfælde sågar umuligt, for myndighederne 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."

Det følger af databeskyttelsesforordningens artikel 23, stk. 1, at rækkevidden af de forpligtelser og rettigheder, der er omhandlet i forordningens artikel 12-22 og 34 samt artikel 5, for så vidt bestemmelserne heri svarer til rettighederne og forpligtelserne i artikel 12-22 kan begrænses ved lovgivningsmæssige foranstaltninger, når en sådan begrænsning respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de forhold, der er oplistet i artikel 23, stk. 1, litra a-j.

Derudover følger det af præambelbetragtning nr. 73 til databeskyttelsesforordningen, at en sådan begrænsning bør være i overensstemmelse med kravene i chartret og i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.

Det råderum, som findes i artikel 23, kan f.eks. anvendes til at fastsætte, at den dataansvarlige efter en konkret vurdering kan gøre visse undtagelser fra reglerne i forordningens artikel 12-22 og 34 samt tilsvarende regler i artikel 5, af hensyn til en eller flere af de interesser, der er oplistet i artikel 23, stk. 1, litra a-j. Det bemærkes, at denne mulighed for så vidt angår artikel 13-14 (om oplysningspligt) og artikel 15 (om indsigtsret) samt artikel 34 (om underretningspligt ved sikkerhedsbrud) allerede er udnyttet i databeskyttelseslovens § 22, stk. 1 og 2.

I bemærkningerne til udkastets § 4 er der henvist til, at det vil være nærliggende at vurdere, hvorvidt en begrænsning af den registreredes rettigheder kan være nødvendig af hensyn til en medlemsstats generelle samfundsinteresser efter databeskyttelsesforordningens artikel 23, stk. 1, litra e.

Det forhold, der fremgår af databeskyttelsesforordningens artikel 23, stk. 1, litra e, er hensynet til andre vigtige målsætninger i forbindelse med beskyttelse af Unionens eller en medlemsstats generelle samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, herunder valuta-, budget- og skatteanliggender, folkesundhed og social sikkerhed.

I bemærkningerne til udkastets § 4 fremgår det følgende endvidere:

> "I den forbindelse er det vurderet, hvorvidt et generelt ressourcehensyn i forbindelse med viderebehandling af allerede indsamlede oplysninger, kan vægtes højere end hensynet til den registreredes rettigheder. Det kan dog ikke antages, at et ressourcemæssigt hensyn alene kan veje op for hensynet til at beskytte den registreredes rettigheder på et generelt plan. Derfor bør ressortministrene overveje, om et ressourcehensyn eller andre relevante hensyn kan gøre sig gældende på deres specifikke

område i en sådan grad, at den registreredes rettigheder kan begrænses eller fraviges."

Datatilsynet bemærker i den forbindelse, at Det Europæiske Databeskyttelsesråd (EDPB) i forhold til artikel 23, stk. 1, litra e, har udtalt, at de omkostninger, der er forbundet med at give oplysninger, og dermed den økonomiske byrde for de offentlige budgetter, ikke er tilstrækkelige til at begrunde en offentlig interesse i at begrænse de registreredes rettigheder.[22]

Det er Datatilsynets opfattelse, at et nationalt retsgrundlag, der begrænser de registreredes rettigheder, skal forholde sig til, hvordan den valgte konkrete begrænsning af rettighederne respekterer det væsentligste indhold af de grundlæggende rettigheder og frihedsrettigheder. Det skal endvidere fremgå, hvordan indskrænkningen er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund, og at begrænsningen alene sker til mindst ét af de forhold, der er nævnt i artikel 23, stk. 1, litra a-j. Herudover skal den lovgivningsmæssige foranstaltning – hvis relevant – som minimum indeholde specifikke bestemmelser om de forhold artikel 23, stk. 2, litra a-h nævner.

Efter Datatilsynets opfattelse stilles der derfor krav om en betydelig klarhed til ethvert nationalt retsgrundlag, der begrænser de registreredes rettigheder.

Det er ikke indlysende for Datatilsynet, at det ved den i udkastet tilsigtede delegation fra lovgiver til samtlige ressortministre er muligt at fastsætte regler i bekendtgørelser, der med den fornødne klarhed overholder de indholdsmæssige krav til den lovgivningsmæssige foranstaltning, der er nævnt ovenfor.

Derudover bemærker Datatilsynet, at det næppe vil være foreneligt med forordningen at fastsætte en generel undtagelse for visse kategorier af dataansvarlige fra helt at skulle iagttage reglerne, ligesom det næppe vil være foreneligt med forordningen at fastsætte en generel undtagelse fra at skulle iagttage disse regler ved specifikke behandlingsaktiviteter i forhold til alle registrerede.

7. Afsluttende bemærkninger

Datatilsynet forudsætter at blive hørt i forbindelse med udarbejdelse af bekendtgørelser og lignende generelle retsforskrifter, som knytter sig til lovudkastet, jf. databeskyttelseslovens § 28.

Kopi af dette brev er sendt til Justitsministeriets Lovafdeling til orientering.

22 Afsnit 3.3.3. i EDPBs retningslinjer 10/2020 om begrænsninger i henhold til artikel 23.