Kommunal- og distriktsdepartementet
Postboks 8112 Dep
0032 OSLO

Deres ref.:	Vår ref.: 22/19102 Saksbehandler: Catrine Stadheim // Rådgivningsseksjonen, Juridisk avdeling	Vår dato: 27.02.2023

NAV Arbeids- og velferdsetatens høringssvar til NOU 2022: 11 Ditt personvern – vårt felles ansvar

Vi viser til høringsbrev fra Kommunal- og distriktsdepartementet datert 11. november 2022. Høringen gjelder Personvernkommisjonens rapport i NOU 2022: 11 Ditt personvern – vårt felles ansvar. Vi takker for fristutsettelsen.

Arbeids- og velferdsetaten (NAV) mener Personvernkommisjonen har skrevet en grundig rapport med mange gode betraktninger som påpeker viktige personvernutfordringer.

Arbeids- og velferdsetaten ønsker særlig å fremheve viktigheten av at personvern blir en del av diskusjonen i drøftelse av andre verdier. Spesielt med tanke på digitaliseringspolitikken mener NAV at det er helt sentralt at personvern blir drøftet når det skal bestemmes hva digitaliseringspolitikken skal være og hvordan den skal gjennomføres. For NAV er det viktig å digitalisere og nyttiggjøre seg ny teknologi for at NAV skal kunne levere på samfunnsoppdraget på en brukervennlig, god og effektiv måte. Det er nødvendig at digitaliseringsstrategien som utvikles er et resultat av avveininger mellom ulike verdier, blant annet personvern. Først når en digitaliseringsstrategi lages gjennom avveininger av ulike hensyn vil det være mulig å finne de beste løsningene. Å finne de beste løsningene vil også legge til rette for å bevare tilliten og legitimiteten i befolkningen.

Våre kommentarer er hovedsakelig knyttet til kommisjonens vurderinger og anbefalinger i kapittel 6 om personvern i den digitale forvaltningen.

Til kapittel 5 Det teknologiske landskapet som påvirker personvernet

NAV // ARBEIDS- OG VELFERDSDIREKTORATET // RÅDGIVNINGSSEKSJONEN, JURIDISK AVDELING
Postadresse: Postboks 354 // 8601 MO I RANA
E-post: arbeids.og.velferdsdirektoratet@nav.no

www.nav.no //

Arbeids- og velferdsetaten stiller seg bak de generelle anbefalingene i kapittel 5. NAV står i en særstilling når det gjelder omfang av behandling av personopplysninger om Norges befolkning, både i kvantum og tid. Det er derfor spesielt viktig å ha en reell og grundig avveiing av teknologisk utvikling i lys av personvernet. Det er en forventning i dagens samfunn til enkle, forståelige og effektive tjenester, gjennom teknologi og digitalisering. Digitalisering kan bidra til å skape store gevinster gjennom bedre tjenester og økt effektivitet, og det kan også ha store gevinster for personvernet om digitaliseringen gjennomføres på en personvernvennlig måte og for å fremme personvern. At både politikere og andre sentrale beslutningstakere har kompetanse og forståelse for teknologi og digitalisering i et personvernperspektiv, er avgjørende for å gjøre de gode beslutningene.

Vi støtter Personvernkommisjonens anbefaling[1] om at det bør være et grunnleggende samfunnsprinsipp at innføringen av inngripende teknologi ikke gjøres uten å ha kartlagt hvilke problemer man faktisk ønsker å løse. Videre at det gjøres grundige vurderinger av om det finnes mindre inngripende veier til målet.

Til kapittel 6 Personvern i den digitale forvaltningen

Anbefalingene om en helhetlig tilnærming til personvern i offentlig forvaltning

Personvernkommisjonen anbefaler at det utarbeides en nasjonal personvernpolitikk. Arbeids- og velferdsetaten støtter Personvernkommisjonen når de uttaler at det er nødvendig med en personvernpolitikk som balanserer digitaliseringspolitikken. Flere av anbefalingene fra kommisjonen tar dette opp i seg, for eksempel:

«Personvernkommisjonen anbefaler at regjeringen utarbeider en helhetlig personvernpolitikk for offentlig forvaltning. Personvernpolitikken må ses i sammenheng med digitaliseringspolitikken og gi føringer for hvordan forvaltningen skal gjøre prinsipielle vurderinger om personvern og sikre at borgernes personvern ivaretas i løsningene som utvikles[...]»[2]*.*

Personvernkommisjonen fremhever mange positive sider av digitalisering av offentlig forvaltning, og skriver blant annet at «*[d]igitalisering kan bidra til en effektiv, brukerorientert og rettssikker offentlig forvaltning, og realiserer viktige samfunnsgevinster*».[3] NAV er enige i dette, og ser digitalisering og bruk av ny teknologi som særlig viktig for å utføre vårt samfunnsoppdrag. Derfor er det viktig at en personvernpolitikk ikke blir stående alene, men blir en del av avveininger mellom samfunnets øvrige behov og verdier på en balansert måte. Samtidig er vi enige i at personvernperspektiver ikke har fått den plassen de bør ha i digitaliseringen av offentlig forvaltning. Vi mener spørsmålene om digitalisering og personvern må løftes opp og bli et viktig og vedvarende tema i den offentlige debatten. Poenget med en personvernpolitikk ikke er at personvernet alltid skal gis forrang. Poenget er at personvernhensyn alltid skal *være med* i vurderinger og beslutningsprosesser. Gjøres

[1] NOU 2022: 11 s. 55
[2] NOU 2022: 11 s. 84
[3] NOU 2022: 11 s. 59

dette riktig mener vi at digitalisering og personvern kan sameksistere og spille hverandre gode. Vi mener innebygget personvern vil kunne bidra til en slik positiv sameksistens, og derfor at politikk som stimulerer til innebygget personvern bør prioriteres.

For å oppnå et godt samspill mellom personvern og andre hensyn mener NAV at samfunnet trenger en modnere forståelse av hva personvern er. Oppfattelsen av personvern bør endres til en forståelse av personvern som en grunnleggende verdi og menneskerett i seg selv, som er en av byggesteinene for både demokrati, ytringsfrihet, tankefrihet osv. Dette skjer ikke primært gjennom etterlevelse av personvernregelverket, men gjennom en personvernpolitikk som tar sin plass i det offentlige ordskiftet.

En personvernpolitikk kan ha forskjellige lag. For det første kan politikken si noe om hva slags beslutninger om personvern den ønsker å befatte seg med. Den kan si noe om når et spørsmål om personvern gjøres til gjenstand for politisk behandling og for eksempel gjennomføres i lov. For det andre, kan politikken si noe om hvordan en beslutning skal spres til de relevante aktørene. Gjennomføring i lov er et eksempel på en type spredning som kan bidra til enhetlig oppfatning og praksis på tvers av forvaltningen, og i samfunnet for øvrig. Dette vil gi en felles retning for forvaltningen. Personvernpolitikk kan sammenlignes med finanspolitikk, eller digitaliseringspolitikk – den er av sektorovergripende natur. Fra innbyggernes perspektiv er det nødvendig at personvern betraktes helhetlig: de trenger en helhetlig beskyttelse. Det hjelper lite hvis én etat beskytter gitte personopplysninger dersom en annen ikke beskytter de samme opplysningene.

For det tredje trenger personvernpolitikken innhold. Det finnes flere eksempler på lovforarbeider som sier at «personvern skal tillegges vekt» eller liknende. I praksis er dette en påminnelse om eksistensen av personvernregelverket. Politikken bør komme med mer - den bør si noe om verdien av personvern, om verdiavveininger der personvern står opp mot eller er samvirkende med andre verdier slik som effektivisering og brukervennlighet. Den bør reflektere over totalbelastningen av behandlinger innbyggerne blir utsatt for, og gi føringer for hvordan de behandlingsansvarlige kan og bør forholde seg til dette. Den kan si noe om hvilket risikonivå som er forsvarlig i risikovurderingene personvernforordningen legger opp til. Den kan si noe om hva slags informasjonsaktivitet en behandlingsansvarlig bør drive. Den kan si noe om hvordan reglene *bør* være og praktiseres.

En personvernpolitikk vil kunne gi en rekke positive ringvirkninger. Den vil kunne øke bevisstheten rundt personvern, noe som vil føre til mer debatt, som igjen vil gi bedre forståelse for alle i samfunnet, inkludert de som er involvert i regelverks-, tjeneste- og digital produktutvikling. Da vil personvernperspektiver bli en mer naturlig del av disse prosessene. Ved å se teknologi og personvern (og digital etikk for øvrig) i sammenheng fra dag én vil vi kunne oppnå gevinstene ved digitaliseringen raskere og med bedre personvern.

En sterk og tydelig digitaliseringspolitikk bidrar til å sette premisser for hvordan virksomheten skal løse sine oppgaver. Personvernvurderingene kan da komme på etterskudd, og blir fort knyttet til *hvordan man bygger løsningen* på en personvernvennlig og lovlig måte - eksempelvis ved å be om hjemler til behandlingsgrunnlag eller implementere personvernfremmende tiltak. De mer grunnleggende personvernvurderinger om *selve*

oppdraget eller handlingen kan da komme for sent. Dette kan føre til at nødvendig behandlingsgrunnlag for å utføre pålagte oppgaver mangler og oppdraget må stanses, eller at man får hjemler uten at grunnleggende personvernvurderinger er tatt. Fravær av en tydelig personvernpolitikk øker sannsynligheten for at slike situasjoner oppstår, og at store og viktige diskusjoner om personvern ikke blir tatt eller ikke blir tatt på riktig nivå.

Personvernkommisjonen mener at en av utfordringene i offentlig forvaltning er begrenset parlamentarisk kontroll og anbefaler at «*Stortinget bør sikres større innflytelse på digitaliseringen av offentlig forvaltning og hvilke konsekvenser dette får for innbyggernes personvern. Involvering av Stortinget bidrar blant annet til at beslutninger blir bedre belyst og får bredere forankring»*[4].

I tråd med norsk lovgivningstradisjon og politisk vilje er NAV, som mange andre etater, gitt vide rammer til å utføre sitt samfunnsoppdrag på den mest hensiktsmessige måten. Både i lovgivning med vide og skjønnsmessige hjemler, og i styringsdokumenter fra departementet, er dette tydelig. Enten aktivitetene rettes etter brukernes (innbyggernes) behov og preferanser eller styres av et mål om å nå flest mulig på en ressurseffektiv måte, har NAV stor fleksibilitet. I tillegg har NAV føringer for sine handlinger gjennom digitaliseringspolitikken.

I hjemlene og digitaliseringspolitikken er det stort sett fravær av personvernvurderinger. Personvernforordningen legger gjennom prinsippene om lovlighet, nødvendighet og proporsjonalitet opp til at en rekke verdivurderinger skal gjøres av den behandlingsansvarlige, som NAV. Spørsmålet er om det i så stor grad er forvaltningsorganet selv som bør avveie hvilke interesser og verdier som skal vike for at organet skal få gjennomført sitt samfunnsoppdrag og digitaliseringsprogram. I NAV gjøres slike vurderinger i personvernkonsekvensvurderinger (DPIA) utarbeidet av forskjellige fag- og utviklingsmiljøer. Dette kan føre til variasjoner i verdivurderinger også internt og en fragmentert tilnærmelse til personvern.

NAV mener at det er grunn til å gi Stortinget større innflytelse på hvordan disse vurderingene og avveiningene gjøres. Vi mener det i større grad bør diskuteres *politisk* hvilke verdier man skal tillegge hvor stor vekt og hvordan disse skal avveies mot hverandre. NAV, og andre offentlige virksomheter, trenger *innhold* til personvernvurderingene de er pålagt å gjøre. En personvernpolitikk kan bidra til slikt innhold.

På særlig viktige områder kan, som kommisjonen foreslår, Stortinget få denne innflytelsen gjennom lovgivningsprosessen:

«Personvernkommisjonen mener tiltak med stor innvirkning på innbyggernes personvern bør hjemles i lov, i stedet for å forskriftsfestes. På den måten får Stortinget muligheten til å ha oversikt over forvaltningens behandling av personopplysninger.»[5]

[4] NOU 2022:11 s. 72

Arbeids- og velferdsetaten støtter forslaget. Lovregulering har flere fordeler. Prosessen er grundigere og gir en bredere politisk forankring og behandling enn en forskriftsprosess. Det kan gi viktige bidrag i utformingen og spredningen av en personvernpolitikk, som beskrevet over. Dette vil både kunne gjøres i selve lovteksten, men ikke minst i lovens forarbeider. Her kan lovgivers vilje kommuniseres.

Hjemmel i lov vil også kunne hjelpe politikerne til å løfte blikket og se sammenhenger på tvers av sektorer. Dette kan være en fordel for eksempel når et politisk tiltak involverer samarbeid på tvers av sektorer og virksomheter. Slike samarbeid kan fort medføre utfordringer når det kommer til deling av data og behandlingsgrunnlag for dette. Et eksempel er arbeidsmarkedstiltaket IPS (individuell jobbstøtte) som ble innført som en forskrift under arbeidsmarkedsloven § 12. Metodikken bak IPS legger opp til et tett og forpliktende samarbeid mellom NAV og helse- og omsorgstjenesten med behov for deling av personopplysninger om en bestemt pasientgruppe med fokus på arbeid uten at behandlingsgrunnlaget er avklart i forkant. Arbeids- og velferdsetaten mener at det før etablering av slike samarbeid på tvers av sektorer bør gjøres de nødvendige juridiske avklaringer av hjemmelsgrunnlag, deling av informasjon og avklaring av behandlingsansvar.

Som tiltak for å styrke en helhetlig tilnærming til personvern i offentlig forvaltning og som del av personvernpolitikken, anbefaler Personvernkommisjonen *«at regjeringen legger frem en personvernpolitisk redegjørelse for Stortinget årlig, forankret i gjeldende personvernpolitikk.»*[6]

NAV støtter forslaget, og mener en årlig personvernpolitisk redegjørelse vil bidra til

- at Stortinget opprettholder fokus på personvern,
- at personvern får større/en plass i det offentlige ordskiftet,
- at Stortinget får et godt bilde av personvernets tilstand i Norge – helhetlig og horisontalt,
- at effekten av personvernpolitikken i stort synliggjøres,
- at det totale trykket av behandlinger av personopplysninger om hver enkelt innbygger synliggjøres og kan vurderes helhetlig.
- at Stortinget kan videreutvikle og justere personvernpolitikken fortløpende,
- at regjeringen og den underliggende forvaltningen, herunder NAV, får og opplever et større ansvar for rapportering av tilstanden på personvernområdet og opplever større eierskap til etterlevelse av regelverk og politiske føringer.

Alt dette vil bidra til en positiv sirkel for personvernet, som vil styrke

- demokratiet, ved at innbyggerne kan følge med på effekten av en personvernpolitikk og hvordan de selv er beskyttet i bruk av deres personopplysninger og dermed får kunnskap til å agere,

---

[5] NOU 2022: 11 s. 84
[6] NOU 2022: 11 s. 84

- innbyggernes tillit til offentlig forvaltning,
- innbyggernes personvern – dersom dette prioriteres,
- forutsigbarhet for virksomheter i offentlig forvaltning,
- mulighet for virksomheter i offentlig forvaltning til å påvirke personvernpolitikken,
- forutsigbarhet for aktører i markedet som leverer tjenester/produkter til det offentlige og
- rettferdiggjørelse av personvernpolitikk og endring av denne, regler og anbefalte retningslinjer.

Anbefaling om et rådgivende og frittstående organ for forvaltningen

Arbeids- og velferdsetaten støtter anbefalingen om et rådgivende og frittstående organ for forvaltningen som kan vurdere og drøfte prinsipielle og generelle spørsmål knyttet til bruk av personopplysninger, herunder samfunnsmessige og etiske spørsmål.[7] Dersom organet kan hjelpe til med å gi innhold til etiske vurderinger og verdivurderinger, vil dette bidra til å styrke og effektivisere personvernvurderinger som gjøres i forvaltningen, herunder hos NAV. I tillegg kan organet ha en viktig stemme i det offentlige ordskiftet, være rådgivende i utforminger av strategier innenfor digitalisering og ved lovgivningsprosesser.

Anbefaling knyttet til forenlighetsvurderinger ved viderebehandling av personopplysninger for å sikre befolkningens tillit

Offentlig forvaltning har et særlig ansvar for å ivareta innbyggernes tillit. Det er viktig at viderebehandling av personopplysninger skjer i tråd med det innbyggerne forventer og er informert om. Personvernkommisjonen påpeker at for å ivareta befolkningens tillit krever det «*grundige vurderinger av om formålet med viderebehandling av innbyggernes personopplysninger er forenlig eller ikke med det opprinnelige innsamlingsformål og hvor stor inngrepet viderebehandling innebærer»*[8]*.* Som tiltak foreslår kommisjonen at disse vurderingene bør offentliggjøres.

Disse forenlighetsvurderingene, som personvernforordningen åpner for, kan være vanskelige og ikke alltid like forutsigbare og tilgjengelige for de registrerte. Vi støtter kommisjonens anbefaling om at det er viktig å avklare hva slags videre bruk som er akseptabel og at slike forenlighetsvurderinger bør offentliggjøres.

Offentliggjøring av forenelighetsvurderinger vil kunne bidra til økt transparens, skape en mulighet for demokratisk kontroll, gi innbyggerne mulighet til å klage på vurderinger som er gjort, gi media og andre mulighet til å kritisere, gi forvaltningen en erfaringsbank av vurderinger og mulighet til å lære på tvers og utvikle en mer enhetlig praksis. Dersom vurderinger som konkluderte med *ikke* forenelig også offentliggjøres, vil det, i fravær av rettspraksis eller andre autorative kilder, kunne være nyttig for å finne ut hvor grensen kan

[7] NOU 2022: 11 s. 84 jf. s. 73
[8] NOU 2022: 11 s. 84

anses å gå. Arbeids- og velferdsetaten mener at det burde utredes om offentliggjøring av forenelighetsvurderinger burde være lovpålagt for forvaltningen.

Dette tiltaket har også en side til temaet deling av personopplysninger mellom forvaltningsorganer.

Anbefalingene knyttet til deling av personopplysninger mellom forvaltningsorganer

Arbeids- og velferdsetaten støtter anbefalingen om at «*den nasjonale adgangen til å skape klarhet i hvem som er ansvarlig for etterlevelse av personvernregelverket, må brukes aktivt*.»[9]. Dette er spesielt viktig, som kommisjonen påpeker, der «*deling av personopplysninger inngår som del av et større samarbeid mellom forvaltningsorganer og hvor uklarhet kan medføre alvorlige personvernkonsekvenser*»[10]. Arbeids- og velferdsetaten mener at samarbeid mellom forvaltningsorgan er viktig. Siden samarbeid er viktig er det sentralt at Stortinget og regjeringen legger til rette for at samarbeidene kan gjennomføres på en god måte i tråd med personvernregelverket. Arbeids- og velferdsetaten har erfaringer med at det er krevende å få avklart ansvarsforhold i større samarbeider hvor det deles personopplysninger. Et eksempel på dette er arbeidsmarkedstiltaket IPSt, som beskrevet over.

Det går mye ressurser til utredninger av hvilket organ som har ansvar for hva, og ofte kan rolle- og ansvarsfordelingene være kompliserte. Det har forekommet at slike avklaringer gjøres etter at samarbeidsavtaler er inngått og samarbeid påbegynt. Ved å fastsette rolle- og ansvarsfordelingen i forskrift eller lov, kan både behandlingsansvar og registrertes rettigheter ivaretas bedre. Et eksempel på hvordan ansvarsfordeling kan fastsettes er høringsnotatet fra Arbeids- og inkluderingsdepartementet[11] om forskrift om felles behandlingsansvar for behandling av personopplysninger i arbeids- og velferdsforvaltningen etter NAV-loven § 14 a. I utkast til forskrift er det forslag om felles behandlingsansvar mellom Arbeids- og velferdsetaten og kommunal del av NAV-kontoret ved innsamling og bruk av personopplysninger etter NAV-loven § 14a.

For samarbeidsformer som er mindre komplekse og har kortere varighet, vil lovfesting av ansvar være mindre aktuelt. Vi slutter oss til kommisjonens anbefaling om at i disse tilfellene vil det kunne bidra til kvalitet og effektiv ressursbruk om det «*utarbeides og videreutvikles standarder for deling av personopplysninger*»[12], som vil gjøre det lettere å samarbeide.

---

[9] NOU 2022: 11 s. 85

[10] NOU 2022: 11 s. 85

[11] Arbeids- og Inkluderingsdepartementet «Høring- Forskrift om felles behandlingsansvar for behandling av personopplysninger i arbeids- og velferdsforvaltningen etter NAV-loven § 14 a» lenke: https://www.regjeringen.no/no/dokumenter/horing-forskrift-om-felles-behandlingsansvar-for-behandling-av-personopplysninger-i-arbeids-og-velferdsforvaltningen-etter-nav-loven-14-a/id2962049/

[12] NOU 2022: 11 s. 85

Standarder for deling av personopplysninger bør inneholde retningslinjer for å kunne dele data effektivt og i samsvar med dataminimeringsprinsippet. Det bør vurderes om det er mulig å lage løsninger hvor man kun deler akkurat de opplysningene som det andre forvaltningsorganet trenger istedenfor for å duplisere informasjonskilder. For eksempel har NAV en egen kopi av folkeregisteret og inntektsopplysninger fra skatteetaten for å kunne hente opplysningene fra disse registrene når etaten trenger det til sin saksbehandling og oppgaveløsning for øvrig. Med dagens systemer er det ikke teknisk mulig å hente opplysningene fra folkeregisteret eller skatteetaten hver gang NAV har lovmessig behov for tilgang til personopplysningene. Arbeids- og velferdsetaten mener at det bør gis ressurser til å lage systemer for deling som kan håndtere den mengden forespørsler.

Gode informasjonskilder som forvaltes på en god måte, er en forutsetning for å sikre at tilgang til personopplysninger kun er mulig etter grundige og dokumenterte vurderinger. Det vil føre til at opplysningene kun blir brukt til det konkrete formålet de er innhentet for, og at gjenbruk (deling) av disse ikke blir synonymt med flytting og/eller lagring (duplisering) flere steder i det offentlige.

Videre mener Arbeids- og velferdsetaten at man burde utrede og politisk bestemme hvordan man skal nå målet om en mer helhetlig tilnærming til deling i forvaltningen. Et eksempel på dette er Personvernkommisjonens anbefaling om at «*regjeringen utreder om en samtykkebasert gjennomføring av «kun-én-gang»-prinsippet vil kunne avhjelpe noen av personvernulempene som oppstår ved deling av personopplysningen mellom offentlige etater».*[13] Arbeids- og velferdsetaten mener at utredningen om «kun-én-gang»-prinsippet bør omfatte mer enn en vurdering av om den kan være samtykkebasert for å kunne avhjelpe eventuelle personvernulemper. Utredningen bør omfatte hvordan «kun-én-gang»-prinsippet kan bli gjennomført på en mer personvernvennlig måte. For eksempel bør utredningen inkludere i hvilken grad innbyggere kan velge å hente sin egen informasjon fra andre offentlige etater, uavhengig av om samtykke er behandlingsgrunnlaget.

Innbyggere bør, i større grad enn hva som er tilfelle i dag, selv kunne råde over i hvilken grad det offentlige skal dele den registrertes data i forbindelse med offentlig tjenesteyting. Som et ledd i å utvikle helhetlige og brukerrettede tjenester har NAV og samarbeidende etater utarbeidet et konsept og prototype for den såkalte «livshendelsen dødsfall og arv». Konseptet legger til grunn at innbygger selv henter dataene fra det offentlige, og sammenstiller disse på sin egen elektroniske enhet, for deretter å simulere om hen kan ha rett til ulike former for tjenester og ytelser fra det offentlige. I fortsettelsen vil innbygger kunne for eksempel “samtykke” til deling av data etatene imellom, for å søke på de konkrete tjenestene og ytelsene.

I forbindelse med deling av data vil Arbeids- og velferdsetaten peke på at det er et behov for å harmonisere regelverket for ulike offentlige etater. Harmonisering av begreper er en del av dette. Harmonisering vil gjøre det enklere å dele personopplysninger på tvers og være med på å sikre bedre datakvalitet og informasjonsbehandling. Det vil også øke

[13] NOU 2022: 11 s. 85

samhandlingsevnen i det offentlige. Dermed vil det være enklere å gjennomføre «kun-én-gang»-prinsippet på en god måte.

Arbeids- og velferdsetaten vil i tillegg peke på at det kan være gode grunner for at Stortinget har en oversikt over og dermed et mer bevisst forhold til hvilke offentlige etater som deler hvilken informasjon seg imellom og til hvilke formål. Det er uheldig at det er overlatt til de enkelte etater eller sektorer å vurdere hvorvidt innsamling, deling og gjenbruk av personopplysninger kan tillates uten at dette er gjenstand for reell parlamentarisk kontroll. Det er liten debatt rundt dette, og liten transparens vanskeliggjør parlamentarisk kontroll. Det er viktig at delingen blir gjennomført på en god og lovlig måte, samt at man tar bevisste valg om hva som blir delt.

God informasjonsforvaltning, med godt beskrevet strukturerte data av høy kvalitet, er en forutsetning for digitalisering. Dette er også en forutsetning for forsvarlig forvaltning herunder godt personvern. God informasjonsforvaltning er også nøkkelen til retten til å bli glemt. Det er vanskelig å sikre sletting når opplysninger spres vidt i ustrukturert form og/eller det er uklart hva opplysningen har blitt brukt til.

Anbefalingene om utforming av lovhjemler

Arbeids- og velferdsetaten støtter alle anbefalingene til kommisjonen knyttet til utforming av lovhjemler.[14] Vi mener at en grundigere vurdering av personvernkonsekvenser i lovarbeid vil føre til lover som i større grad tar hensyn til personvern. Dette inkluderer for eksempel vurderinger av hvor inngripende loven er i personvernet og hvordan kravene til klarhet etter EMK, Grunnloven og personvernforordningen oppfylles. Personvernkonsekvensvurderinger i lov- og forskriftsarbeid er viktig av tre grunner:

1. For innbyggernes forutberegnelighet og dermed tillit til forvaltningen. For Arbeids- og velferdsetaten er forutberegnelighet for innbyggere spesielt viktig fordi vi møter mange innbyggere i vanskelige livssituasjoner. I tillegg er innbyggere ofte avhengig av NAV for å ha penger til livsopphold. Avhengigheten til NAV og situasjonen borgerne er i gjør at det er ekstra viktig for oss at lovene er klare slik at vi kan drive på en tillitsvekkende måte.

2. For å etterleve generelt regelverk som Grunnloven, personvernregelverket og forvaltningsretten samtidig som vi oppfyller kravene i særlovgivning. Om personvern ikke er vurdert når en lov utarbeides kan handlingen loven pålegger være delvis i konflikt med personvern. Vi har skrevet mer om disse konfliktene under punktet om helhetlig personvernpolitikk, hvor vi fremhever viktigheten av at politiske mål blir nedfelt i lov.

[14] NOU 2022: 11 s. 84-85

3. Når det er tatt hensyn til personvern i lovarbeid, vil det være mindre krevende for forvaltningen å finne ut av hva som faller innenfor og utenfor lovene. Det vil altså være enklere for forvaltningen å anvende lovene. Klarere lover og forskrifter er viktig for oss for å oppnå effektivisering og bedre tjenester, og for å i større grad å sikre at valgene som blir tatt er innenfor lovverket. Vår erfaring fra digitalisering er at det er svært mye arbeid knyttet til tolkning for å forstå hvordan vi på lovlig vis kan levere på samfunnsoppdraget.

Klarere lover og forarbeider er også sentralt for samarbeid og deling av informasjon mellom forvaltningsorganer. Dette er fordi det vil være varierende kapasitet og ressurser til arbeid med personvern. Vi har skrevet mer om utfordringer ved samarbeid i punktet om deling av informasjon i offentlig sektor.

For å få bedre personvernkonsekvensvurderinger i lovarbeid og lover som i større grad tar hensyn til personvern, har Personvernkommisjonen pekt på helt sentrale virkemidler i anbefalingene sine på s. 84-85 om "Utforming av lovhjemler".

Til slutt er det en grunnleggende forutsetning for å kunne gjennomføre personvernkonsekvenser i lovarbeidet at personvernkompetansen i forvaltningen styrkes. Dette er viktig på alle nivåer - fra departement til alle deler av etater som deltar i utarbeidelse av lov og forskrifter.

Anbefalingen om styrking av personvernkompetansen

Vi er enige i kommisjonens anbefaling om at offentlig forvaltning må styrke personvernkompetansen til ledere og saksbehandlere og at det bør inngå i den obligatoriske grunnopplæringen for nyansatte.[15]

Arbeids- og velferdsetaten har obligatorisk grunnopplæring i personvern for alle nyansatte, inkludert ledere. Den enkelte medarbeiders kunnskap og kompetanse er en sentral forutsetning for å lykkes med etterlevelse av personvernkrav. Etatens ledere har en nøkkelrolle fordi det er et lederansvar å sørge for at egne medarbeidere har tilstrekkelig kompetanse, og at de selv også har kunnskap om hva deres ansvar for personvern innebærer i praksis. Det er også viktig at personvernkompetansen holdes jevnlig oppdatert.

Digitaliseringen av forvaltningen åpner mange nye problemstillinger hvor det ennå ikke finnes presedensavgjørelser, konsensus eller beste praksis, eksempelvis hvordan man kan ivareta den registrertes interesserer, autonomi, vernet mot diskriminering, krav til åpenhet m.m. i møte med kunstig intelligens. Det finnes få tilbud som sikrer faglig kompetansepåfyll for jurister som jobber med digital produktutvikling, og det kan være ekstra krevende å navigere i et felt som utvikler seg så raskt. Vi etterlyser derfor også tilbud som styrker spesialistkompetansen i skjæringsfeltet mellom juss og digital teknologi i offentlig forvaltning.

[15] NOU 2022: 11 s. 84-85

Anbefalinger knyttet til bruk av kunstig intelligens (KI)

Bruk av kunstig intelligens og maskinlæringssystemer trekkes frem av Personvernkommisjonen som et av områdene innenfor teknologiutviklingen som utfordrer personvernet. Som påpekt i rapporten kan bruk av maskinlæring/kunstig intelligens være et både nyttig og effektiviserende verktøy i offentlig sektor. Samtidig reiser bruk av denne teknologien en rekke juridiske og etiske utfordringer knyttet til beskyttelse av menneskerettigheter og den enkeltes rett til personvern. Vi ønsker også å påpeke at størrelsen av inngrepet og utfordringene ved bruk av kunstig intelligens kan være ulike. For eksempel vil bruk av maskinlæring til automatiske beslutninger eller til kontrollformål være inngripende, mens mindre inngripende bruk av KI kan være å hjelpe veiledere med å raskere finne relevant informasjon til brukerne.

Vi støtter overordnet kommisjonens beskrivelse av mulighetene og utfordringene ved bruk av maskinlæring i offentlig forvaltning,[16] samtidig som vi mener det er grunnleggende og viktige problemstillinger som ikke er berørt i rapporten, men som bør inngå i en videre utredning av tematikken, herunder hvordan utvikling og bruk av maskinlæring i offentlig forvaltning bør innrettes og reguleres. Under gir vi eksempler på slike problemstillinger, som vi løfter frem for å synliggjøre kompleksiteten i problemstillingene og dermed behovet for en grundigere utredning.

Om maskinlæring og automatisert rettsanvendelse

Personvernkommisjonen fastslår at maskinlæring ikke kan benyttes til å automatisere rettsanvendelse. Vi er uenige i denne slutningen: selv om maskinlæring ikke kan benyttes til juridisk fortolkning, eller å uttrykke tolkningsresultatene som programkode, kan en tenke seg at faktagrunnlaget som inngår i et tolkningselement hentes fra et statistisk beregningsverktøy som maskinlæring. Et eksempel på dette kan være maskinlæringsbasert estimering av ligningsverdi, som inngår i en programmatisk skatteberegning. Selv om maskinlæringens funksjonelle rolle ikke er å tolke lover og regler, eller prøve vilkår, kan den likefult inngå som et element i et system hvor regelverkstolkninger er operasjonalisert gjennom programkode som utføres automatisk av en maskin. Også en ved en slik bruk av maskinlæring kan det hefte personvernproblemstillinger som fortjener en bredere debatt. Det sentrale spørsmålet er ikke hvorvidt rettsanvendelse handler om statistiske beregninger eller ikke, men snarere om – og i så fall når – statistiske beregninger kan eller ikke kan benyttes som grunnlag i en rettsanvendelse.

Om maskinlæring i beslutningsstøttesystemene

Selv om kommisjonen peker på noen utfordringer knyttet til ukritisk bruk av slik maskinlæringsbasert beslutningsstøtte, mener vi en slik bruk reiser noen fundamentale problemstillinger som fortjener grundigere utredning:

- Det er rimelig å anta at forvaltningsorganer ønsker å benytte maskinlæringsbaserte beslutningstøtter fordi forslagene antas å være riktige og med et ønske om å dreie saksbehandlingspraksis i en mer enhetlig og ønsket retning. Når blir så en

[16] NOU 2022: 11 s. 64-65

beslutningsstøtte et de facto beslutningssystem? Når blir forslagene for vektige for det endelige vedtaket?
- En maskinlæringsmodell kan forholde seg til flere informasjonselementer enn en manuell saksbehandler, men hvilke elementer skal inngå og hva er å regne som utenforliggende hensyn i rettslig forstand?
- Hva betyr det for rettsikkerheten at maskinlæringsmodell og saksbehandler både ser ulike informasjonselementer og vektlegger disse ulikt i samme sak? Maskinlæringsmodellen kan vektlegge et sett med kriterier for å komme frem til sin anbefaling, mens saksbehandler kan benytte anbefalingen og vektlegge andre informasjonselementer i endelig begrunnelse? Hvordan kan slike forskjeller ettergås?

Om maskinlæring og profilering
Kommisjonen fastslår at maskinlæring er godt egnet til profilering, som kan gi opphav til såkalt «gruppe-til-individ-problem», som følger når slutninger om en enkeltperson foretas basert på egenskaper til en gruppe. Det diskuteres imidlertid ikke om bruk av algoritmisk profilering i offentlig forvaltning øker risikoen for at enkelte (sårbare) grupper blir gjenstand for gjentatte personverninngripende behandlinger på tvers av ulike offentlige aktører, og hvorvidt individvernet bør suppleres med et rettslig gruppevern. Også slike spørsmål bør etter vårt syn vurderes i en eventuell regulering av maskinlæring i offentlig forvaltning.

Problemstillinger fra NAVs prosjekt i Datatilsynets regulatoriske sandkasse
Flere nye utfordringer som har relevans også for andre deler av offentlig forvaltning og som derfor bør ses på når man vurderer innretning og regulering av kunstig intelligens, blir belyst gjennom NAVs deltakelse[17] i Datatilsynets regulatoriske sandkasse:
- Maskinlæring forutsetter typisk behandling av personopplysningene om andre, for å skaffe til veie en ny personopplysning om den registrerte. Når, og eventuelt under hvilke forhold, bør det åpnes for denne typen behandlinger?
- Maskinlæring (for beslutningsstøtteverktøy) forutsetter typisk en behandling av større mengde personopplysninger, enn saksbehandling uten maskinell beslutningsstøtte. Når, og under hvilke omstendigheter, bør det åpnes for denne typen behandlinger?
- Utvikling av maskinlæringsmodeller kan ofte forutsette trening på historiske personopplysninger til enkeltpersoner som ikke lenger er i en relasjon til den offentlige virksomheten. Når, og under hvilke omstendigheter, bør det åpnes for denne typen behandlinger?

Etatens prosjekt, som var å utvikle et KI-verktøy for å gjøre oppfølgingen av sykmeldte mer brukervennlig og effektiv, ble lagt på is på bakgrunn av Datatilsynets konklusjon om at NAV hadde rettslig grunnlag til å kunne *bruke* KI til beslutningsstøtte, men at det derimot var usikkert om det rettslige grunnlaget åpnet for bruk av personopplysninger til å *utvikle* og trene algoritmer. Datatilsynet anbefaling var at det var nødvendig med et klart og tydelig rettsgrunnlag for utvikling og at dette burde avklares gjennom en lovprosess med tilhørende

[17] NAV sluttrapport, januar 2022, Datatilsynet og NOU 2022: 11 s. 67

høringsrunde og utredninger. Øvelsen i sandkassen har synliggjort en viktig utfordring som trolig gjelder på tvers av offentlig virksomheter: lovene som hjemler behandling av personopplysninger, er sjeldent utformet på en måte som åpner, eller setter klare skranker for bruken av personopplysninger til maskinlæring i offentlig forvaltning. Usikkerheten forsterkes av fraværet av presedens, konsensus og ulike regelverk og ulik tolkningspraksis på tvers av offentlige virksomheter.

Arbeids- og velferdsetaten slutter seg til kommisjonens anbefaling om rettslig regulering av utvikling og bruk av kunstig intelligens/maskinlæring, og vi mener at dette arbeidet bør prioriteres og utredes nærmere. Dette må sees i sammenheng med den kommende KI-reguleringen (forordning for kunstig intelligens). Videre slutter vi oss til anbefalingen i kapittel 9[18] om viktigheten av at regjeringen engasjerer seg i utforming av forordningen med vedlegg og arbeider for en utvikling som sikrer at KI-systemer utformes på en måte som ivaretar personvernet i både utvikling og bruk av slike systemer. Hvordan kunstig intelligens/maskinlæring bør reguleres vil være en viktig del av innholdet i en helhetlig personvernpolitikk. Tematikken fortjener en grundig utredning og bred offentlig debatt, herunder også på hvilke områder der personvernlovgivningen muligens kommer til kort i å gi tilstrekkelige rettsikkerhetsgarantier.

En slik utredning må vurdere om utvikling og bruk av kunstig intelligens må lovreguleres særskilt, hva som skal reguleres og hvor detaljert reguleringen skal være, samt om det bør reguleres i særlovgivning og/eller for eksempel forvaltningsloven. Slike spørsmål er helt sentrale for forutberegneligheten til innbyggerne i møte med den digitale forvaltningen. Det foreligger i dag ingen konsensus eller veiledning rundt hvordan tematikk som transparens, forklarbarhet, likebehandling, diskriminering, m.m. skal forstås rettslig eller håndheves i praksis i offentlig forvaltning. Den regulatoriske sandkassen til Datatilsynet er et av få verktøy offentlige virksomheter har for å utforske nye problemstillinger og mulige løsninger som oppstår i skjæringspunktet mellom personvern og maskinlæring. Sandkassen er imidlertid ingen arena for tverretatlig erfaringsutveksling eller enhetlig rettsforståelse og praksis på tvers av offentlige virksomheter. Utvikling og utrulling av maskinlæring i offentlige virksomheter bør være tuftet på et felles etisk rammeverk, og gi innbyggeren en forutsigbarhet i hvordan rettssikkerhetsmekanismer er iverksatt.

Vi etterlyser derfor tydeligere føringer, skranker og krav til etterlevelse for utvikling og bruk av maskinlæring med personopplysninger i offentlig forvaltning. Kravene bør følges opp med veiledning om hvordan rettssikkerhetsprinsippene kan ivaretas.

Anbefalingene om profilering til kontrollformål

Arbeids- og velferdsetaten støtter Personvernkommisjonens anbefaling om at «*profilering for å avdekke ulovligheter alltid bør sees som en inngripende behandling som krever solid hjemmel i lov*» og «*at offentlig forvaltning burde anvende føre-var-prinsippet ved bruk av profilering til kontrollformål*»**.**[19]

[18] NOU 2022: 11 s. 181

[19] NOU 2022: 11 s. 80

Lintvedt har i vedlegget til kommisjonens rapport[20] påpekt at NAV har vide hjemler for kontroll og at disse innebærer profilering gjennom utplukk til kontroll. I rapporten skriver kommisjonen i punkt 6.4.5 at «*det kan ikke overlates til etatene selv å utforme nærmere kriterier og retningslinjer for innsamling og bruk av personopplysninger for profileringsformål som har inngripende virkninger. At forvaltningen kan innhente nødvendige opplysninger om noe som kan være relevant for bredt formulerte formål, gir i denne sammenheng ikke tilstrekkelig rettsbeskyttelse og forutberegnelighet for innbyggerne*».

Vi er enige i at Arbeids- og velferdsetatens hjemler for kontroll er vide, og ser at det kan utfordre personvernet for innbyggerne. Dagens hjemler er et resultat av sterk politisk vilje til å forebygge og avdekke trygdemisbruk, uten at personvernkonsekvenser ble drøftet grundig i forarbeidene. Det har siden den tid kommet ny teknologi som kan påvirke vurderingen av kontroll opp mot personvern og som foranlediger en diskusjon om temaet. Vi er som nevnt over enige med kommisjonen i at profilering for å avdekke ulovligheter alltid bør sees som en inngripende behandling som krever solid hjemmel i lov. En del av avveiningene mellom blant annet personvern- og kontrollhensyn som vi må gjøre i forbindelse med dette regelverket er etter vårt syn avveininger som med fordel kunne vært tatt på politisk nivå. Vi mener at det er viktig med et forutsigbart regelverk, spesielt i lys av hvor inngripende en kontroll er i seg selv.

I en videreutvikling av regelverket må det gjøres vurderinger av hvor tungt hensynet til personvern skal veie opp mot myndighetenes behov for kontroll. Fremtidige kontrollhjemler må være utformet på en slik måte at de tar høyde for et kriminalitetsbilde i stadig endring og som samtidig ivaretar hensynet til personvernet. Vi mener at en personvernpolitikk som løfter opp diskusjonen om utforming av kontrollhjemler og tiltak i offentlig forvaltning vil være nyttig.

Anbefalingene om offentlige aktører og store teknologiselskaper

Arbeids- og velferdsetaten mener personvernpolitikken, når den utformes, bør reflektere over det offentliges bruk av store teknologiselskaper. Som Personvernkommisjonen påpeker kan det fort skapes et avhengighetsforhold til disse selskapene som det er vanskelig å fri seg fra, ettersom det finnes få alternative tjenestetilbydere. Slik de store teknologiselskapene opptrer i dag, kan det være vanskelig å etterleve personvernregelverket når man bruker tjenestene deres. Virksomhetene, som har ansvar for å etterleve regelverket, blir stående i en skvis: på den ene siden skal de etterleve, på den andre siden trenger de verktøyet. For mange er det ikke mulig å opprettholde drift uten verktøyene. Derfor får man i praksis en situasjon der teknologiselskapene i stor grad dikterer premissene, selv om disse både kan være i gråsonen og også utenfor regelverket. Arbeids- og velferdsetaten mener at det offentlig bør stå mer samlet i anskaffelser av verktøy fra store teknologiselskaper for å kunne anskaffe nødvendige verktøy som også er i tråd med regelverket.

I tillegg til etterlevelsesperspektivet, kommer det etiske perspektivet: Er det riktig at teknologiselskapene skal ha så mye makt?

[20] Lintvedt, M. N. (2022). Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering. Utredning for personvernkommisjonen.

En av kommisjonens anbefalinger gjelder sosiale medier. Det tar opp i seg både etterlevelsesperspektivet og det etiske perspektivet: «*Personvernkommisjonen mener offentlige virksomheter må gjøre grundige vurderinger av om de skal benytte sosiale medier for å gi informasjon og kommunisere med innbyggere. Sosiale medier bør ikke brukes i konkret enkeltsaksbehandling*». [21] Arbeids- og velferdsetaten støtter anbefalingen. Sosiale medier slik de ser ut i dag er stort sett eid av store teknologiselskaper med en forretningsmodell som baserer seg på innsamling og videresalg av brukernes personopplysninger. Vi er enig i at offentlige virksomheter må gjøre grundige vurderinger om de skal benytte slike tjenester. Samtidig erfarer vi at dette på flere plan er svært utfordrende vurderinger, og mener at dette er noe som det burde gis veiledning om i en personvernpolitikk.

Personvernkommisjonen virker å ville stille strengere krav når det kommer til offentlige virksomheters *egne* nettsteder enn når det kommer til nettsteder som eies av andre, men som det offentlige opptrer på – slik som nettsteder for sosiale medier. Det uttales i kapittel *6.4.6.1 Særskilt om sporing på offentlige nettsteder* at offentlig sektor ikke skal «*betale for analyseverktøy og andre tjenester ved å utlevere innbyggernes personopplysninger*».[22] Det bør også gjøres til et politisk spørsmål om bruken av *andres* nettsteder bør betraktes mildere enn bruken av *egne* nettsteder, når andres nettsteder brukes av offentlig sektor. Vi har over sett at betalingen for bruk av mange av de sosiale mediene nettopp skjer med innbyggernes personopplysninger. Likevel er anbefalingen kun at virksomhetene burde gjøre grundige vurderinger på sosiale medier, mens på egne nettsider uttales det at man bør avstå fra å betale med innbyggeres personopplysninger.

Tiltaket om å *«tilgjengeliggjøre informasjon til innbyggerne i digitale løsninger der personopplysninger samles inn og brukes av kommersielle aktører til kommersielle formål, som for eksempel til å bygge og berike profiler eller deles med tredjeparter»*,[23] er en følge av informasjonsplikten etter personvernforordningen og er slik sett ikke nytt. Det er likevel viktig at det faktisk gjøres. Samtidig kan det stilles spørsmål ved om tiltaket er egnet, dersom målet er å ikke betale for tjenester ved å utlevere innbyggernes personopplysninger.

«Personvernkommisjonen mener det er viktig at det gjøres både personvern – og datastrategiske vurderinger når det offentlige benytter tjenester fra store teknologiskaper. Fordi spørsmålene ofte er likelydende, bør forvaltningen samarbeide på tvers av sektorer og nivåer for å sikre høy faglig kvalitet og god bruk av ressurser».[24] Dette tar opp i seg flere av problemstillingene nevnt over. Arbeids- og velferdsetaten understreker viktigheten av at slike grundige vurderinger gis innhold gjennom en personvernpolitikk. Vurderingene fører til avgjørelser som påvirker samfunnet på et bredt plan og bør ha politisk forankring.

[21] NOU 2022: 11 s. 85
[22] NOU 2022: 11 s. 82
[23] NOU 2022: 11 s. 85
[24] NOU 2022: 11 s. 85

Til kapittel 11 Teknologi i personvernets tjeneste

Arbeids- og velferdsetaten støtter anbefalingen om å skape tydeligere plikter til innebygget personvern.[25] Dette vil gjøre etterlevelse for virksomheter mindre komplisert. I tillegg vil det kunne hjelpe virksomheter med å stille krav til leverandører i anskaffelser, samt bedre kunne evaluere hva leverandørene tilbyr. Leverandørene vil kunne få et sterkere initiativ til å levere tjenester med innebygget personvern i og med at kundene er pålagt klare regler for etterlevelse. Det vil også gi leverandørene større forutsigbarhet i og med at det vil være lettere å avgjøre hvilke tiltak de må gjennomføre for å oppnå innebygget personvern i det produktet eller den tjenesten de leverer. Disse fordelene vil også gjelde virksomheter som utvikler egne tjenester og produkter.

Arbeids- og velferdsetaten har både stor egenutviklingstakt og er en stor innkjøper i markedet. De fleste av etatens behandlinger er også hjemlet i de behandlingsgrunnlag kommisjonen mener kan gi grunnlag for tydeligere og mer konkrete plikter. Slik sett vil etaten kunne dra nytte av tiltaket.

Arbeids- og velferdsdirektoratet stiller i dag krav til innebygget personvern til tilbydere i anskaffelsesprosesser. Men det kan oppleves som utfordrende å vurdere hvor konkrete og strenge kravene skal være, og deretter hvilke tiltak hos tilbyderne/leverandørene som skal anses som gode nok eller hvor mye de skal veie sett opp mot andre krav i anskaffelsen. Anskaffelseskravene om innebygget personvern har sitt grunnlag i personvernforordningen artikkel 25. Kravene i artikkel 25 er meget skjønnsmessige. Den skjønnsmessige karakteren gjør det vanskelig å sette tydelige og klare krav i anskaffelsesprosesser. Det kan føre til at innebygget personvern blir prioritert ned sammenlignet med andre anskaffelseskrav hos begge parter.

I og med at klarere krav til innebygget personvern vil gjøre det lettere å være tydelige ovenfor leverandører (og interne utviklere, besluttere, innkjøpere etc.), vil dette være et verktøy for å bidra til *det foreslåtte tiltaket om stimulering til utvikling av norsk personvernteknologi*.[26] Dette er også et tiltak Arbeids- og velferdsetaten støtter.

Felles anbefalte anskaffelseskrav for offentlig sektor vil også gjøre det lettere å stille de riktige kravene og evaluere besvarelsene av dem.

Forslaget til kommisjonen om å innta plikter for innebygd personvern i ny forvaltningslov[27] vil gi hele forvaltningen et felles utgangspunkt og vil bidra til å synliggjøre pliktene for samfunnet for øvrig – både for tjenesteleverandører og innbyggerne. NAV støtter derfor forslaget.

Andre anbefalinger

[25] NOU 2022: 11 s. 201 pkt. 11.5 andre strekpunkt.
[26] NOU 2022: 11 s. 201 pkt. 11.5 siste strekpunkt.
[27] NOU 2022: 11 s. 201

Vi slutter oss til anbefalingene i de øvrige kapitlene 10, 12 og 13. Til kapittel 10 vil vi spesielt trekke frem at det er sentralt med forståelige regler for innbyggerne. Mer forståelige regler vil også gjøre arbeidet for forvaltningen enklere. Videre vil vi trekke frem at forvaltningen har behov for å bygge opp ytterliggere kompetanse innen EU/EØS-rett.

Til kapittel 12 om åpenhet er vi enig med kommisjonens i at Digitaliseringsdirektoratets rapport om «Innsynsløsning – tekniske og juridiske muligheter» (2022) inneholder en rekke interessante og gode forslag som bør følges opp av Kommunal- og distriktsdepartementet. Mange av forslagene til tiltak vil kunne være med på å understøtte innbyggernes behov for mer helhetlig informasjon og oversikt over forvaltningens behandling av personopplysninger.

Arbeids- og velferdsetatens slutter seg til anbefalingene i kapittel 13 om å styrke Datatilsynet på informasjons- og veiledningssiden. Når andre myndigheter utarbeider veiledninger om personvernspørsmål mener vi det er viktig at Datatilsynet er med i utarbeidelsen. Dette bidrar til å sikre veiledningene kvalitet og legitimitet. Datatilsynet bør ha tilstrekkelige ressurser og kapasitet til å bistå i personvernkonsekvensvurderinger og i lov- og forskriftssaker. Dette er viktig for å bedre kvaliteten både på personvernkonsekvensvurderinger og i regelverksarbeid der det er høy risiko for registrertes grunnleggende rettigheter og friheter. Videre slutter vi oss til anbefalingen om at Datatilsynets sandkasse for kunstig intelligens videreføres. Sluttrapportene fra de ulike prosjektene i sandkassen har blitt viktige kilder for kunnskap og veiledning samt at prosjektene og kommunikasjonen rundt disse har bidratt til å løfte viktige dilemma og problemstillinger.

Med hilsen

Hans Christian Holte
arbeids- og velferdsdirektør

Dette dokumentet er godkjent elektronisk og har derfor ingen signatur