

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse
19/2580 EO TRR/bj

Vår referanse
19/01698-2/JHN

Dato
02.12.2019

Høringsuttalelse – NOU 2019: 5 Ny forvaltningslov

Vi viser til høringsbrev av 03.06.2019 om NOU 2019: 5 Ny forvaltningslov.

Generelle merknader

NOU 2019:5 er omfangsrik og grundig. Det er gledelig at sentrale problemstillinger på personvernområdet er drøftet. En økt digitalisering av offentlig forvaltning åpner for en mer effektiv saksbehandling, men utfordrer også den enkeltes personvern.

Vi har i vår høringsuttalelse fokusert på utredningens kapittel 18 om automatiserte beslutningsprosesser, og kapittel 19 om deling av personopplysninger mellom forvaltningsorganer. Dette er komplekse temaer som kommer til å være en sentral del av den digitale forvaltningen i fremtiden. Vi mener dette krever en bredere vurdering enn det som er gjort i utredningen.

I personvernforordningen er det nedfelt sentrale prinsipper om at all behandling av personopplysninger skal være lovlig, rettfærdig og åpen. Disse prinsippene må være førende for en ny forvaltningslov som skal ivareta den enkeltes rettsikkerhet i et digitalt samfunn. Et viktig utgangspunkt er at den enkelte skal ha kontroll over egne personopplysninger. Automatiserte beslutningsprosesser og deling av personopplysninger mellom forvaltningsorganer utfordrer disse prinsippene, og det er derfor helt nødvendig å utrede disse temaene grundig.

For at den enkelte selv skal kunne være i stand til å ivareta sine rettigheter og medvirke til en rettsikker forvaltning, må man tenke helhetlig omkring disse spørsmålene. Det gjelder alt fra innhenting av opplysninger, datakvalitet og kvalitetssikring av beslutningssystemer til kontradiksjon, begrunnelse og tilsyn med eventuell strukturell forskjellsbehandling, for eksempel diskriminering som utilsiktet kan bli kodet inn i systemene.

Personvernkonsekvensene av lovforslaget er ikke vurdert i utredningen, noe som er en plikt etter personvernforordningen art. 35. Forordningen legger spesielt vekt på at personvernkonsekvensvurderinger må gjennomføres ved innføring av ny teknologi. Dette vil særlig gjelde ved innføringen av helautomatiserte beslutningsprosesser. For å ivareta den demokratiske kontrollen med forvaltningen, må Stortinget få forelagt informasjon som gjør at

det kan ta stilling til påregnelige konsekvenser og risiko ved å innføre hjemler som kan yte stor påvirkning på personvernets stilling i Norge.

Det følger av personvernforordningen art. 36 nr. 4 at medlemsstatene skal rådføre seg med tilsynsmyndigheten ved utarbeiding av forslag til lovgivning som skal vedtas av et nasjonalt parlament, eller av et reguleringstiltak som er basert på slik lovgivning, og som er knyttet til behandling av personopplysninger. Denne plikten inntreffer dersom vurderingen av personvernkonsekvenser i medhold av art. 35 konkluderer med at forslaget sannsynligvis vil medføre høy risiko for den registrertes rettigheter og friheter. Regelen i art. 36 nr. 4 innebærer at slik forhåndskonsultasjon må gjennomføres før lovforslaget sendes ut på ordinær høring. Dette er en plikt som følger av personvernforordningen, og en eventuell unnlattelse vil kunne innebære et brudd på personvernforordningen, og dermed også Norges EØS-rettslige forpliktelser.¹

I dette høringsvaret er det ikke mulig å komme med løsninger på alle de problemstillinger som en ny forvaltningslov og en digital forvaltning fører med seg, men Datatilsynet ønsker å bidra til at vi får en effektiv, moderne og rettssikker forvaltning, samtidig som vi sørger for å ivareta personvernet.

Konklusjoner

Datatilsynets høringsuttalelse kan oppsummeres ved hjelp av følgende konklusjoner:

- Det må gjennomføres en utredning av personvernkonsekvenser, spesielt vedrørende kapittel 18 om automatiserte beslutningsprosesser, og om kapittel 19 om deling av personopplysninger mellom forvaltningsorganer.
- Terminologien mellom personvernforordningen og ny forvaltningslov må harmoniseres.
- Forslagets §§ 11 og 12 om automatiserte beslutningsprosesser må utredes grundigere.
- Forslagets § 36 om deling av personopplysninger mellom forvaltningsorganer må utredes grundigere.
- Datatilsynet må forhåndskonsulteres før lovforslaget oversendes Stortinget, jf. personvernforordningen art. 36 nr. 4.

Rettslig utgangspunkt

Retten til privatliv er en grunnleggende forutsetning for et fritt demokratisk samfunn. Rettigheten er nedfelt i Grunnloven § 102, EMK art. 8 og FNs internasjonale konvensjon om sivile og politiske rettigheter (SP) art. 17.

EMK art. 8 oppstiller skranker for hvilke inngrep staten kan gjøre i borgernes privatliv. Inngrep i denne rettigheten må tilfredsstille de krav som følger av disse bestemmelsene og praksis i Den europeiske menneskerettsdomstol (EMD).

¹ Sml. den britiske regjeringens veiledning om art. 36 nr. 4 <https://www.gov.uk/government/publications/guidance-on-the-application-of-article-364-of-the-general-data-protection-regulation-gdpr/guidance-on-the-application-of-article-364-of-the-general-data-protection-regulation-gdpr>

Staten må etter denne bestemmelsen vurdere hvorvidt et konkret tiltak vil medføre en begrensning av noens rett til privatliv, om begrensningen er i samsvar med loven, og om begrensningen er nødvendig i et demokratisk samfunn. Helt sentralt står lovskravet, som krever at å begrense noens rett til respekt for sitt privatliv må være hjemlet i nasjonal lov. Lovskravet innebærer både at det skal foreligge en nasjonal lov som regulerer inngrepet, og et krav til lovens kvalitet: lovgivningen må være tilstrekkelig klar og forutberegnelig. Dette kravet har som formål å verne mot vilkårlige inngrep fra myndighetene. Jo større inngrepet er, jo strengere må kravet tolkes. Loven må altså være klar og forståelige nok, slik at den gjengse borger, om enn med rådgivning, kan forutse sin rettsposisjon.

En begrensning av individuelle rettigheter må også forfølge legitime formål og være nødvendig i et demokratisk samfunn. Dette betyr at det må foretas en avveining mellom samfunnets/statens interesse og inngrepet i retten til privatliv. Det må derfor vurderes både fordeler og ulemper ved tiltaket. Dette for å fastslå om inngrepet i privatlivet er forholdsmessig.

I dette ligger det et krav om at staten må vurdere hvorvidt det er iverksatt egnede tiltak for å gjøre begrensningen i en rettighet så lite byrdefull som mulig. I vurderingen av om dette kravet er oppfylt, må lovgiver se hen til hvordan dette er regulert i lov, men også hvordan dette fungerer, eller vil komme til å fungere, i praksis.

Personopplysningsloven, som gjennomfører personvernforordningen, setter rammer for nasjonal lovgivning, og stiller krav til at den enkeltes rettigheter og friheter blir ivaretatt. Det er åpenbart at borgernes samhandling med forvaltningen innebærer utveksling av opplysninger som er nødvendig for å kunne gjennomføre de oppgaver forvaltningen er pålagt, og for å sikre borgernes rettigheter.

Likevel oppstår det utfordringer som kan medføre at retten til privatliv ikke i tilstrekkelig grad blir ivaretatt. Datatilsynet er spesielt opptatt av automatiserte beslutningsprosesser og deling av informasjon mellom forvaltningsorganer.

Kapittel 18 om automatiserte beslutningsprosesser

Det er foreslått to bestemmelser som omhandler automatiserte beslutningsprosesser. En ny § 11 om helautomatisert saksbehandling, og § 12 om automatiserte saksbehandlingssystemer. Innledningsvis er det grunn til å påpeke at bestemmelsenes overskrifter er noenlunde likelydende, og det bør fremgå at § 12 er et dokumentasjonskrav.

Til ny § 11 om helautomatisert saksbehandling har flertallet foreslått følgende bestemmelse:

«Kongen kan gi forskrift om at forvaltningsorganet på bestemte sakområder kan treffe avgjørelser ved helautomatisert saksbehandling. Avgjørelser som er lite inngripende overfor den enkelte, kan treffes ved helautomatisert behandling uten hjemmel i forskrift.»

Mindretallet har foreslått:

«Forvaltningsorganet kan treffe helautomatiserte avgjørelser hvor personopplysninger inngår, når behandlingen er nødvendig for å utøve offentlig myndighet eller utføre lovfestede oppgaver. Behandlingen må sikre partens krav til forsvarlig saksbehandling og være forenlig med retten til vern av personopplysninger.»

Hovedhensyn og utgangspunkter

Utgangspunktet er at det foreligger en rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, (...) jf. personvernforordningen § art. 22 nr. 1, og at helautomatisk behandling forutsetter at vilkårene i art. 22 nr. 2 bokstav b er oppfylt.

Blant annet må staten gjennomføre egnede tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser.

I art. 22 nr. 3 er det oppstilt noen minstekrav for hva som regnes som egnede tiltak når det gjelder bokstav a og c, men disse kravene må anses relevante også for bokstav b:

- retten til menneskelig inngripen fra den behandlingsansvarlige
- den registrertes rett til å uttrykke sine synspunkter
- den registrertes rett til å bestride avgjørelsen

Det europeiske personvernrådet (EDPB) har gitt konkrete anbefalinger om slike tiltak i sine «Retningslinjer om automatiske individuelle avgjørelser og profilering i henhold til forordning 2016/679» (WP 251 rev.01), se nedenfor.²

I tillegg stilles det krav til ytterligere tiltak i art. 22 nr. 4, som omhandler behandling av særskilte kategorier personopplysninger. Bestemmelsen viser blant annet til art. 9 nr. 2 bokstav g, som krever særlige tiltak på grunn av innholdet i personopplysningene hvor de særskilte kategoriene inneholder mer sensitive opplysninger. Behandlingen må også være nødvendig av hensyn til viktige allmenne interesser, og den må stå i et rimelig forhold til det mål som søkes oppnådd. Dette er ikke behandlet i utredningen.

Det er grunn til å påpeke at manglende gjennomføring av egnede tiltak etter personvernforordningen kan innebære brudd på våre EØS-forpliktelser.

Flertallet legger opp til at reglene som utvalget foreslår om kontradiksjon, begrunnelse og klageadgang, trolig er tilstrekkelige for å vareta forordningens krav til å fastsette egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser.

Det er grunn til å stille spørsmål ved om dette tilfredsstiller kravet i personvernforordningen.

² Retningslinjene ble utarbeidet av Artikkel 29-gruppen, men disse ble «endorsed» av EDPB den 25. mai 2018, se «Endorsement 1/2018» <https://edpb.europa.eu/node/89>

Prosessuelle rettigheter overfor forvaltningen må anses som minimumsgarantier, og det må derfor måtte kreves andre tiltak som er egnet til å redusere den økte risiko en automatisert behandling anses å medføre (se EDPBs retningslinjer).

Man må også vurdere om lovgrunnlaget her vil være klart nok formulert. Det vil være vanskelig å identifisere hva art. 22 nr. 2 viser til når ikke de særskilte tiltakene uttrykkelig er formulert i lovteksten, spesielt retten til menneskelig inngripen, som er noe annet enn klagerett, og dermed ikke følger av utkastets generelle saksbehandlingsregler.

Loven bør også slå fast at ved klage på automatisert vedtak, så skal klagen alltid behandles av mennesker. Klagebehandlingen bør ikke bare være en kontroll med at programlogikken er fulgt, men en reell behandling av sakens faktiske og rettslige sider.

Flertallet foreslår også et skille mellom avgjørelser som er lite inngripende for den enkelte, som skal kunne treffes uten hjemmel i forskrift, og mer inngripende avgjørelser, som vil måtte hjemles i forskrift.

For mindre inngripende avgjørelser vil da grunnlaget for å gjøre unntak fra hovedregelen i art. 22 nr. 1 basere seg på formuleringen om at inngripende avgjørelser må hjemles i forskrift, noe som er lite presist.

Det gjøres ikke rede for hvor dette skillet går og det er en svakhet ved forslaget. Når dette ikke er klart formulert, så kan det argumenteres med at lovgrunnlaget ikke er tilstrekkelig klart nok for å gjøre unntak fra rettighetene, som må ivaretas uansett hvor inngripende avgjørelsen er.

Det kan tenkes at en heller bør gjøre et skille mellom avgjørelser som er fullt ut regelstyrte, og de som inneholder et element av skjønn.

Datatilsynet mener at flertallets forslag ikke i tilstrekkelig grad ivaretar hensynet til den enkeltes mulighet til å ivareta sine rettigheter og friheter etter personvernforordningen.

Mindretallets forslag innebærer en generell hjemmel til å helautomatisere saksbehandlingen uten å stille ytterligere krav enn det som følger av personvernforordningen og forvaltningsloven. I forslaget kreves det at behandlingen må være nødvendig for å utøve offentlig myndighet eller utføre lovfestede oppgaver, samt at behandlingen må sikre krav til forsvarlig saksbehandling og være forenelig med retten til vern av personopplysninger.

Dette er en form for sirkelargumentasjon hvor mindretallets forslag til ny forvaltningslov § 11 peker tilbake på forvaltningsloven, og indirekte på personvernforordningen og de krav som følger av den. I og med at art. 22 nr. 2 krever at det skal fastsettes egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser, vil da forvaltningslovens tiltak være å henvise til personvernforordningen.

Det sentrale hensynet bak plikten til å gjennomføre tiltak i § art. 22 nr. 2-4 er å sikre en demokratisk diskusjon og forankring før man iverksetter helautomatiske beslutningsprosesser, noe en generell hjemmel ikke ivaretar.

Datatilsynet vurderer det slik at ingen av forslagene tilfredsstiller kravene i personvernforordningen art. 22 om egnede og særskilte tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser.

Det kan argumenteres for at tiltakene kan gjennomføres i særlovgivning, men sett i lys av betydningen av forvaltningsloven, så bør det nedfelles prinsipper som er førende for all helautomatisert saksbehandling.

Etter Datatilsynets vurdering, så krever disse spørsmålene en bredere vurdering enn det som er foretatt i utredningen.

Det bør blant annet sies noe om vurdering av personvernkonsekvenser (DPIA), minimumsrettigheter og vurdering av risiko. Dette er en lov som forhåpentligvis skal leve lenge, og det er viktig at den tar opp i seg de utfordringer som ny teknologi, blant annet bruk av kunstig intelligens og maskinlæring vil medføre.

Datatilsynet vil likevel komme med et forslag til hvordan en lovbestemmelse kan utformes, slik at den bedre ivaretar den enkeltes rettigheter. Det er grunn til å påpeke at bokstav c har sitt grunnlag i personvernforordningen art. 36 nr. 4 og innebærer en forhåndskonsultasjon før forslaget sendes ut på høring. Dette er en plikt som følger av personvernforordningen. Som nevnt vil en eventuell manglende forhåndskonsultasjon kunne innebære et brudd på våre EØS-forpliktelser.

«(1) Kongen kan gi forskrift om at forvaltningsorganet på bestemte sakområder kan treffe avgjørelser ved helautomatisert saksbehandling.

(2) Før forvaltningsorganet/Kongen fastsetter eller endrer en forskrift om helautomatisert saksbehandling, skal det

a) alltid utrede personvernkonsekvensene

b) vurdere egnede og særlige tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser

c) konsultere Datatilsynet på forhånd dersom vurdering av personvernkonsekvenser tilsier at behandlingen vil medføre en høy risiko for fysiske personers rettigheter og friheter og berettigede interesser.

(3) Enhver har rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på helautomatisert saksbehandling, og rett til menneskelig inngripen fra den behandlingsansvarlig

Eksempler på tiltak

For en ytterligere redegjørelse for hvilke tiltak som kan gjennomføres viser Datatilsynet til [WP251 - Retningslinjer om automatiske individuelle avgjørelser og profilering i henhold til forordning 2016/679](#).

I veilederen drøftes blant annet de mer generelle garantiene i personvernforordningen som utredning av personvernkonsekvenser, retten til informasjon, retten til å korrigere og slette etc. I tillegg foreslås det tiltak som kan falle inn under art. 22.

Eksempler på dette er (sitert fra dansk oversettelse):

- regelmessige kvalitetssikringskontroller av deres systemer for at sikre, at de registrerte behandles rimelig og ikke forskjelsbehandles, enten på grunnlag av særlige kategorier av personopplysninger eller annet grunnlag
- algoritmisk audit – testning av de algoritmer, der anvendes og utvikles av maskinlæringsystemer, for at påvise, at de rent faktisk fungerer etter hensikten og ikke gir diskriminerende, feilagtige eller uberettigede resultater
- i forbindelse med uafhængig tredjemandsaudit (hvis beslutningstagning baseret på profilering har stor indvirkning på enkeltpersoner) – tilveiebringelse af alle de nødvendige oplysninger om, hvordan algoritmen eller maskinlæringsystemet fungerer, til revisoren
- opnåelse af kontraktlige garantier for tredjepartsalgoritmer om, at audit og testning er udført, og at algoritmen er i overensstemmelse med vedtagne standarder
- specifikke foranstaltninger til dataminimering med henblik på at fastlægge klare opbevaringsperioder for profiler og for alle personoplysninger, der anvendes i forbindelse med oprettelse eller anvendelse af profilerne
- anvendelse af anonymiserings- eller pseudonymiseringsteknikker i forbindelse med profilering
- udvikling af metoder, der giver den registrerede mulighed for at fremkomme med sine synspunkter og bestride afgørelsen
- en mekanisme for menneskelig indgriben i nærmere bestemte tilfælde, f.eks. ved at angive et link til klageadgang, når den registrerede informeres om den automatiske afgørelse, med fastlagte frister for fornyet gennemgang og et navngivet kontaktpunkt, der kan besvare eventuelle spørgsmål.
- certificeringsmekanismer for behandlingsaktiviteter
- adfærdskodekser for revisionsprocesser vedrørende maskinlæring
- etiske evalueringspaneler, der skal vurdere de potentielle samfundsmæssige skadevirkninger og fordele forbundet med bestemte anvendelser af profilering.

§ 12 Dokumentasjonskrav - Automatiserte saksbehandlingssystemer

Datatilsynet støtter en bestemmelse om å dokumentere det rettslige innholdet i automatiserte saksbehandlingssystemer, og anser det som helt nødvendig for å kunne ivareta borgernes rettssikkerhet.

Det innebærer imidlertid en meget stor utfordring å gjøre det rettslige innholdet i denne type systemer tilgjengelig på en måte som gjør at borgerne kan nyttiggjøre seg det, og at det tilfredstiller lovskravets krav til at lovgivningen må være tilstrekkelig klar og forutberegnelig.

Utvalget har tatt utgangspunkt i personvernforordningens regler om informasjon i art. 13 nr. 2 bokstav f.

Utvalget drøfter om det er tilstrekkelig at det rettslige innholdet dokumenteres i en kravspesifikasjon basert på pseudokode supplert med naturlig språk. Et enkelt eksempel på pseudokode kan være:

```
hvis <betingelse>
  gjør noe;
ellers
  gjør noe annet;
```

Det er en reell mulighet for at dokumentasjonen kan bli svært omfangsrik og vanskelig tilgjengelig, og i de tilfellene man benytter maskinlæring og kunstig intelligens, så vil beskrivelsene av selve algoritmene ikke nødvendigvis gi tilstrekkelig veiledning for å forstå hva beslutningen faktisk bygger på.

Dette er problemstillinger som i større grad må utredes. Datatilsynet vil vise til § 10 i utkast til ny lov om arkiv i [NOU 2019:9](#), som gir bedre føringer for hvordan denne dokumentasjon bør utformes, og som er mer i samsvar med de felles europeiske retningslinjer som er uttrykt i WP251.

Det åpner også for spørsmål om hvordan reglene i utkastets § 48 om begrunnelse skal utformes. Hvordan begrunner man et vedtak som er et resultat av helautomatisert saksbehandling? Datatilsynet kan ikke se at dette har blitt problematisert. Ved bruk av kunstig intelligens, så bør begrunnelsen også omfatte de vurderinger som er gjort maskinelt.

Bestemmelsen bør også inneholde en plikt til å gjennomføre er uavhengige og periodiske gjennomganger av programlogikk, i alle fall for mer kompliserte algoritmer. Ved bruk av kunstig intelligens så må man må man aktivt og jevnlig teste for *bias* og diskriminering ved hjelp av en uavhengig tredjepart.

Kapittel 19 Deling av taushetsbelagte opplysninger med andre forvaltningsorganer

Det er foreslått å endre adgangen til å dele taushetsbelagte opplysninger med andre forvaltningsorganer som i vesentlig grad svekker den enkeltes personvern.

I forslaget § 36 så åpnes det for deling som legger betydelig mer vekt på hva som er i mottakerorganets interesse.

«(2) Taushetsplikt etter §§ 33 og 34 er heller ikke til hinder for at opplysningene deles med

(...)

c) personer i andre forvaltningsorganer så langt det er nødvendig for å utføre de oppgaver som er lagt til avgiverorganet eller mottakerorganet

(...)

(3) Opplysninger om personlige forhold kan bare deles dersom det er nødvendig og ikke utgjør et uforholdsmessig inngrep overfor den opplysningen gjelder

I en digital forvaltning så vil hensynene til en effektiv saksbehandling og personvern stå både sammen og mot hverandre, noe som utvalget drøfter. I utredningen behandles også rettslig grunnlag og formålsbegrensningsprinsippet. Også her må prinsippet om kontroll over egne opplysninger være retningsgivende.

Slik lovforslaget er utformet, åpner det for en meget omfangsrik deling av opplysninger, uten at denne delingen gjenspeiles i nødvendig kontroll som ivaretar den enkeltes rettigheter.

En svakhet ved utkastet er at det ikke berører flere sentrale problemstillinger som er avgjørende for at personvernet i tilstrekkelig grad blir ivare tatt.

Beslutningskompetanse for deling

Utgangspunktet i personvernforordningen er at både avgiverorganet og mottakerorganet må ha et behandlingsgrunnlag for å kunne dele, dvs. utlevere, personopplysninger til hverandre. Dette innebærer at det alltid ligger beslutningskompetanse hos avgiverorganet. Det fremgår ikke av lovutkastet, selv om det omtales i utredningen. Dette bør klargjøres i den endelige lovteksten.

Informasjon om behandling

Et av de sentrale personvernprinsippene er prinsippet om åpenhet. Prinsippet kommer i forordningen blant annet til uttrykk i konkrete rettighetsbestemmelser om informasjon ved behandling av personopplysninger, og i reglene om rett til innsyn i personvernforordningen.

Når det gjelder utlevering til andre offentlige organer etter § 7-3, så vil det kunne utløse informasjonsplikt etter art. 13 og 14 for avgiverorganet, samt også pålegge mottakerorganet en informasjonsplikt etter art. 14.

Det er mulig å gjøre unntak fra denne informasjonsplikten etter art. 14 nr. 5. De unntakene som kunne tenkes å være relevante i denne sammenhengen, er:

- når den registrerte allerede har informasjonen
- dersom det viser seg umulig å gi nevnte informasjon eller det vil innebære en uforholdsmessig stor innsats
- dersom innsamling eller utlevering er uttrykkelig fastsatt i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt, og som inneholder egnede tiltak for å verne den registrertes berettigede interesser

Slik Datatilsynet forstår forslaget, uten at informasjonsplikten direkte er omtalt, så vil informasjonsplikten kunne unntas med hjemmel i særlovgivning, under forutsetning av at det fastsettes egnede tiltak for å verne den registrertes interesser.

Når omfanget av deling og eventuelle unntakshjemler blir så stort at det blir umulig å holde oversikt, blir det problematisk (sml. forordningen art. 12). Det vil kunne oppstå nærmest uendelige rekker av behandlinger, hvor personopplysninger utleveres til ett forvaltningsorgan som igjen utleverer til et annet, og kobler man inn automatiserte beslutningsprosesser, profilering og kunstig intelligens, så har man ikke lenger bare en sort boks hvor man ikke helt vet hva som skjer med opplysningene inne i boksen, men et forvaltningsmessig sort hull som suger til seg all informasjon uten at man vet hva som kommer ut på den andre siden – satt litt på spissen.

Dette berører en grunnleggende utfordring for hvordan en digital forvaltning må bygges opp fra grunnen. For at den enkelte skal ha kontroll over sine opplysninger, og for å oppfylle legalitetsprinsippet og dets krav om klarhet, så må forvaltningen bygge på prinsippene om innebygd personvern. Innebygd personvern stiller krav til hvordan opplysninger samles inn, kategoriseres og behandles. Det må integreres gjennomsiktighetsmekanismer som innebærer at alle personopplysninger kan spores tilbake til deres kilder, på et hvilket som helst tidspunkt i behandlingen. Det må også stilles også krav til datakvalitet.

Det må klargjøres hvilke prinsipper som gjelder for deling etter anmodning, tilgang eller automatisk – noe som innebærer store forskjeller når det gjelder personvernet.

Forvaltningsloven må derfor fastsette prinsippene for deling av opplysninger på en måte som i større grad klargjør hvordan den enkeltes rettigheter skal ivaretas. Det må klargjøres i hvilken form beslutninger om deling og eventuelle unntak fra informasjonsplikten skal gjøres i og hvordan dette praktisk skal løses, slik at den enkelte har en reell mulighet til å ivareta sine rettigheter. Dette er viktig for at tilliten til staten opprettholdes. Selv om skillet mellom den digitale borger og den digitale stat på mange måter hviskes ut, så er det derfor enda mer viktig at det ligger klare rettslige føringer som grunnlag. I et bondesamfunn var f.eks.

eiendomsretten reell, men i stor grad definert lokalt og geografisk, med unntak av skattefutures årlige besøk, mens i et digitalt samfunn så er berøringspunktene nærmest kontinuerlige.

Det er ikke realistisk eller ønskelig at hver enkelt skal måtte føre kontroll med at opplysningene som deles er korrekte. Det er en for stor oppgave, og man må derfor kunne stole på at det finnes systemer som gjør både forvaltningens og den enkeltes kontroll mulig. Et eksempel nylig er manglende tilbakebetaling av skatt til 17 500 NAV-brukere. Her bestod svikten i at Skatteetaten og NAV ikke hadde gode nok systemer for å fange opp tilbakebetaling av forhåndsbetalt skatt for trygd som ikke skulle vært utbetalt. Dette er noe for så vidt den enkelte kunne ha fanget opp ved å kontrollere skattemeldingen, men ordningen med forhåndsutfylt skattemelding og høy tillit til offentlige myndigheter gjør at mange ikke sjekker tallene. Det er viktig at den samfunnsmessige effektiviseringsgevinsten av digitalisering ikke reduseres av minkende tillitt til forvaltningen og dermed reduserer bruken av digitale tjenester.

Profilering

Datatilsynet vil kort kommentere at det kan tenkes at det bør utformes egne regler for profilering på samme måte som for automatiske beslutningsprosesser. En utfordring vil kunne være der hvor man benytter profilering til for eksempel å velge ut tilsynsobjekter. Her er det viktig å kontrollere at profileringen ikke gjentar iboende fordommer eller svakheter, slik at enkelte individer eller grupper rammes urettmessig.

Det kan også oppstå problemer omkring deling av profiler, innsyn og kontradiksjon og korrigerende av uriktige resultater.

Kapittel 14 Forskrifter

Det er i § 14 foreslått en utredningsplikt for forskrifter. Datatilsynet vil minne om rådføringsplikten som følger av art. 36 nr. 4. Ved utarbeidelse av lovgivning eller forskrift, så skal Datatilsynet i noen tilfeller rådføres utover det som følger av det ordinære høringsinstituttet.

Plikten inntreffer der dersom en vurdering av personvernkonsekvenser i henhold til art. 35 tilsier at behandlingen vil medføre en høy risiko for fysiske personers rettigheter og friheter etter personvernforordningen.

Dette må sees i sammenheng med plikten til å foreta en vurdering av personvernkonsekvenser etter art. 35. nr. 1 hvor det særlig er lagt vekt på bruk av ny teknologi.

Datatilsynet ser det derfor som nødvendig, spesielt med innføring av automatiske beslutningsprosesser, deling av opplysninger, profilering og bruk av kunstig intelligens, så bør kravet til vurdering av personvernkonsekvenser og rådføringsplikt med Datatilsynet presiseres i lovteksten.

Terminologi

Datatilsynet vil også poengtere at forslaget terminologi ikke i tilstrekkelig grad er harmonisert med personvernforordningen. Dette kan medføre tolkningsproblemer og en uklar rettsstilling.

I forslaget brukes § 33 brukes betegnelsen taushetsplikt om «personlige forhold», som igjen viser til opplysninger om en person som det er vanlig å ville holde for seg selv, og som blant annet kan gjelde genetiske eller andre sensitive biometriske forhold, helsetilstand, livssyn eller politisk ståsted, seksuell legning.

I utgangspunktet bør man unngå å bruke skjønsmessige begreper som «vanlig» i tilknytning til personlige forhold, da det kan variere fra miljø til miljø og det kan endres over tid.

Personopplysninger er definert i personvernforordningen art. 4 nr. 1 som «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet»

Det kan synes som om «personlige forhold» i stor grad omhandler det som er definert som særlige kategorier i personvernforordningen art. 9 nr. 1.

I § 35 nr. 1 bokstav b, så gjøres det unntak fra taushetsplikten for «Opplysninger som ... gjelder personer ... som ikke kan identifiseres», som skiller seg fra hvordan dette er definert i personvernforordningen art. 4 nr.1.

Også definisjonen av samtykke i § 36 «gyldig og informert samtykke» skiller seg fra personvernforordningens definisjon i art. 4 nr. 11.

Det endelige utkastet bør gjennomgå, slik at terminologien er lik og gjennomtenkt. Dette illustrerer også en utfordring ved automatiserte beslutningsprosesser. Det er vanskelig å lage presise systemer som lar seg kontrollere hvis man ikke klarer å lage rettsregler som er mulig å sammenlikne.

Konklusjon

Digital forvaltning i form av automatiserte beslutningsprosesser og deling av opplysninger er områder som er i rask utvikling og hvor samfunnet har liten erfaring. Det er derfor behov for en dyptgående utredning av disse spørsmålene.

Dette er komplekse problemstillinger, hvor det er behov teknologisk, juridisk og samfunnsvitenskapelig kompetanse for å komme frem til rettferdige og praktiske løsninger som ivaretar borgernes tillit til staten.

Datatilsynet ber om at rådgøringsplikten etter personvernforordningen art. 36 nr. 4 benyttes og at tilsynet involveres i de relevante delene av lovutkastet.

Personvernkonsekvensene av forslaget må utredes jf. personvernforordningen art. 35.

Datatilsynet vil også minne om Regjeringens beslutning om å nedsette en personvernkommissjon som blant annet skal se på hvordan personvernet kan sikres ved økt bruk av digitale løsninger.

Etter Datatilsynets erfaring, så er Norge langt fremme når det gjelder bruk av digitale løsninger. Ved å benytte seg av dette i lovarbeidet har vi også mulighet til å lage en lov som kan være et eksempel for andre land.

Med vennlig hilsen

Jørgen Skorstad
Avdelingsdirektør

Jan Henrik Nielsen
Juridisk seniorrådgiver