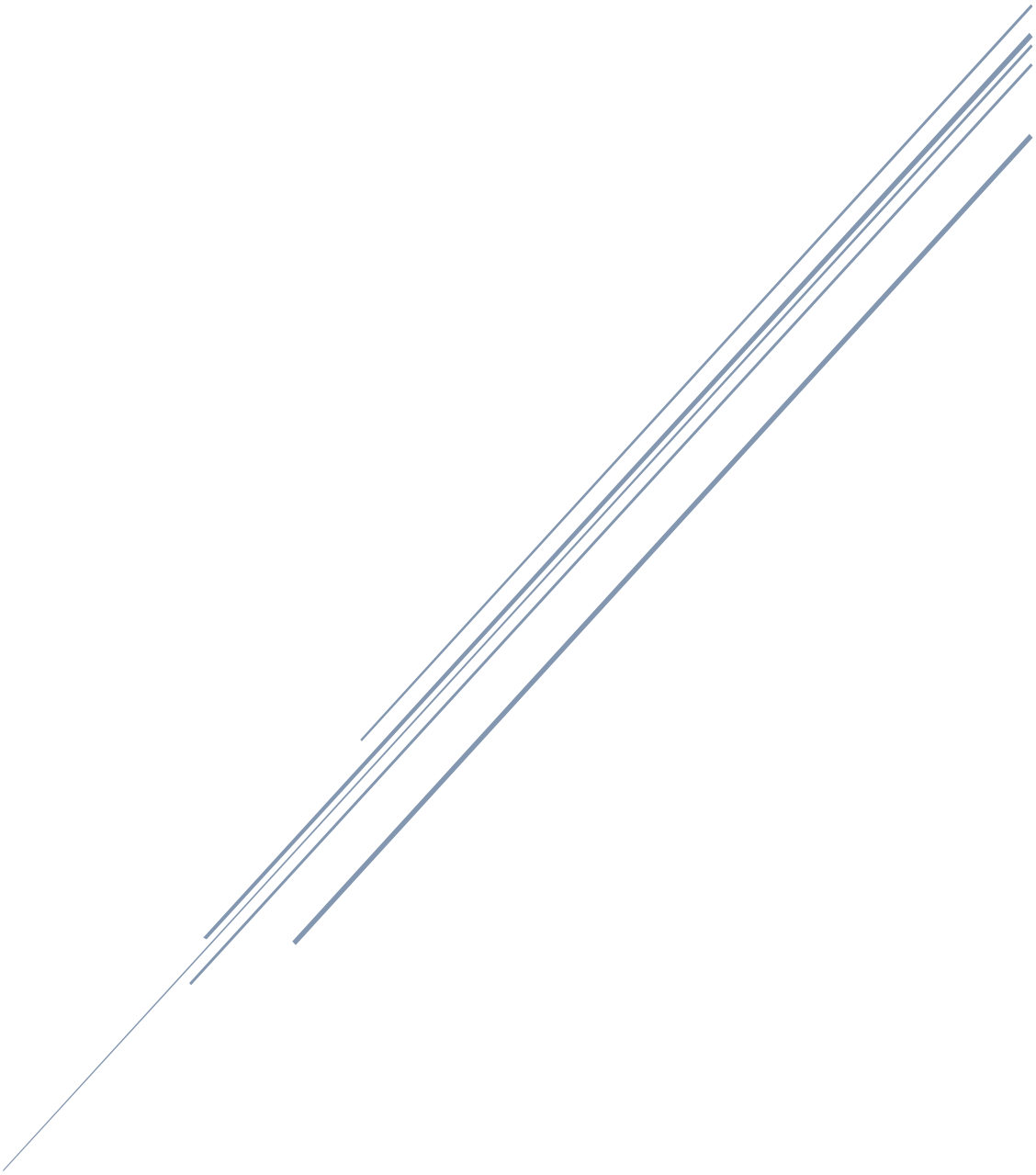
HØRINGSNOTAT

Forskrift om felles behandlingsansvar for behandling av personopplysninger i arbeids- og velferdsforvaltningen etter NAV-loven § 14 a



Arbeids- og inkluderingsdepartementet

Innhold

1. Bakgrunn og hovedinnhold

Arbeids- og velferdsforvaltningen[1] forvalter en rekke velferdsytelser, tilbyr velferdstjenester og hjelper personer som har behov for bistand for å kunne delta i arbeidslivet. For å kunne ivareta oppgavene behandler[2] arbeids- og velferdsforvaltningen et stort antall personopplysninger som skal behandles i henhold til krav i personvernlovgivningen. Med sikte på å tydeliggjøre behandlingsansvaret for behandling av personopplysninger som gjøres etter § 14 a i lov om arbeids- og velferdsforvaltningen (NAV-loven)[3], fremmer Arbeids- og inkluderingsdepartementet forslag til ny forskrift som regulerer dette behandlingsansvaret.

NAV-loven § 14 a gir alle som ønsker eller trenger bistand til å komme i arbeid rett til en systematisk vurdering av sitt bistandsbehov for å komme i arbeid. Vurderingen tar utgangspunkt i personens ressurser og muligheter på arbeidsmarkedet, og gjøres av veiledere på NAV-kontoret. Resultatet av vurderingen utgjør grunnlaget for hvilke tjenester som kan tilbys i et eventuelt oppfølgingsløp, både fra kommunal og statlig side. For å kunne foreta disse vurderingene, behandler arbeids- og velferdsforvaltningen en rekke personopplysninger.

Personvernregelverket stiller krav om klare ansvarsforhold når personopplysninger behandles. Departementet mener at dette ikke er tilstrekkelig tydelig og forutsigbart regulert for behandlingene som skjer i forbindelse med vurderinger etter NAV-loven § 14 a. Det bidrar både til å skape usikkerhet om ansvaret til aktørene som er involvert i behandlingene, og om de registrertes rettigheter etter personvernsregelverket blir tilstrekkelig ivaretatt. For å tydeliggjøre behandlingsansvaret slik at det får en klar, tilgjengelig og forutsigbar ramme, vil departementet regulere dette i egen forskrift med hjemmel i NAV-loven § 3 andre ledd siste setning.

Departementet vurderer at behandlingsansvaret for personopplysninger etter NAV-loven § 14 a er lagt til arbeids- og velferdsforvaltningen, det vil si både kommunene og Arbeids- og velferdsetaten. Behandlingsansvaret for personopplysningene anses å være felles, men med ulik ansvarsfordeling mellom statlig og kommunal side. Blant annet vil Arbeids- og

[1] Arbeids- og velferdsforvaltningen består av Arbeids- og velferdsetaten og de delene av kommunens tjenester som inngår i de felles lokale kontorene (NAV-loven § 2).

[2] «Behandler» omfatter all bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter (https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/)

[3] NAV-loven § 14 a. Vurdering av behov for bistand for å beholde eller skaffe seg arbeid og rett til aktivitetsplan
Alle som henvender seg til kontoret, og som ønsker eller trenger bistand for å komme i arbeid, har rett til å få vurdert sitt bistandsbehov. Brukere som har behov for en mer omfattende vurdering av sitt bistandsbehov, har rett til å få en arbeidsevnevurdering. Brukeren skal få en skriftlig vurdering av

a. sine muligheter for å komme i arbeid
b. hva slags arbeid som skal være målet
c. behovet for bistand for å komme i arbeid
d. om, og eventuelt hvor mye, arbeidsevnen er nedsatt
e. hvilken type bistand som kan være aktuell for brukeren

velferdsetaten ved Arbeids- og velferdsdirektoratet ha ansvaret for IT-løsningene som benyttes i § 14 a-vurderingene.

Departementet vil i dette høringsnotatet belyse forhold som er lagt til grunn for vurderingene og den nye forskriften som foreslås.

2. Dagens regler

2.1 Personvernregelverket

2.1.1 Personopplysningsloven og personvernforordningen

Europaparlaments- og rådsforordning (EU) 2016/679[4] skal styrke og harmonisere personvernet ved behandling av personopplysninger i EU og EFTA-/EØS-området. Forordningen er gjort til norsk lov gjennom personopplysningsloven § 1, med de tilpasninger som følger av vedlegg XI protokoll 1 av avtalen.[5]

Personvernforordningens virkeområde er begrenset til behandling av personopplysninger. Forordningens artikkel 4 nr. 2 definerer behandling:

> *«enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring»*

Behandling av personopplysninger er teknologinøytralt og kan skje både elektronisk og gjennom manuell behandling.

Aktuelle behandlingsgrunnlag for å behandle personopplysninger er omtalt i en uttømmende liste i personvernforordningen artikkel 6, samt i artikkel 9 når det gjelder behandling av særlige kategorier av personopplysninger.

Etter personvernforordningen skal det utpekes en eller flere behandlingsansvarlige som skal ha det overordnede ansvaret for å overholde personvernprinsippene og personvernregelverket (personopplysningsloven og personvernforordningen).

Personvernforordningen artikkel 4 nr. 7 definerer behandlingsansvarlig:

> *«en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes*

[4] Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR]

[5] Bestemmelsene i forordningen går i tilfelle konflikt foran bestemmelser i andre lover, jf. personopplysningsloven § 2 fjerde ledd.

nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett»

Behandlingsansvaret er knyttet til spesifikke behandlingsaktiviteter. Det er de reelle forholdene knyttet til hvordan formål og midler er fastsatt som er avgjørende for ansvarsplasseringen, og dette må vurderes konkret.

Å fastlegge hvem som er behandlingsansvarlig vil enten bero på at det er fastsatt i lov og forskrift, eller på en vurdering av hvem som bestemmer formål og midler med behandlingen av personopplysningene, jf. personvernforordningen. Behandlingsansvaret kan fordeles på tre måter:

- hos *én* aktør
- *delt* mellom to eller flere (her er partene *alene* ansvarlig for ulike deler av behandlingen)
- *felles* mellom to eller flere aktører

2.1.2 Vilkår for at det skal foreligge felles behandlingsansvar

Personvernforordningen artikkel 26 nr. 1 fastsetter at to eller flere behandlingsansvarlige er felles behandlingsansvarlige hvis de i fellesskap fastsetter formålene med og midlene for behandlingen. Dette supplerer den generelle definisjonen av behandlingsansvarlig i artikkel 4 nr. 7. Midler for behandlingen i denne sammenhengen kan være IT-løsninger, men det kan også være organisering og rutiner som påvirker behandlingen.

En forutsetning for å kunne ha et felles behandlingsansvar er at alle de ansvarlige må ha et rettslig grunnlag for behandlingen. Å etablere eller konstatere et felles behandlingsansvar medfører dermed ikke en videre eller annen adgang til å behandle personopplysninger enn hva den enkelte behandlingsansvarlige alene har adgang til på egen hånd.

Det er ikke et krav til de felles behandlingsansvarlige at ansvaret dem imellom er likt fordelt. Felles behandlingsansvar kan ha ulike former og ulik innbyrdes ansvarsfordeling. Det kan også dekke situasjoner hvor én behandlingsansvarlig bare i liten grad er delaktig i å fastsette formål og midler for behandlingen. Dette i motsetning til situasjoner der den ene parten har behandlingsansvaret, og den andre behandler personopplysninger på vegne av den første.

Et sentralt hensyn bak reglene om felles behandlingsansvarlige er å sikre en tydelig ansvarsfordeling, slik at personvernet ikke svekkes når to eller flere behandlingsansvarlige er involvert i behandlingen. Gjennom klarhet om ansvarsforholdene reduseres risikoen for ansvarspulverisering og manglende etterlevelse og kontroll. Det er derfor et selvstendig krav i personvernforordningen artikkel 26 at det må finnes en formalisert regulering av det respektive ansvaret hver behandlingsansvarlig har. En slik regulering kan følge av unionsretten eller medlemstatenes nasjonale rett. Hvis verken unionsretten eller nasjonal rett har regulert forholdet, må ansvaret fastsettes gjennom en ordning mellom de behandlingsansvarlige.

Fordelingen av ansvaret internt mellom de behandlingsansvarlige kan tillegges vekt ved vurderingen av retten til å kreve regress ved erstatningsansvar etter

personvernforordningen artikkel 82, samt ved utmålingen av eventuelt overtredelsesgebyr etter personvernforordningen artikkel 83.

Den interne fordelingen av ansvaret hver behandlingsansvarlig har, endrer likevel ikke at det utad kan være et solidaransvar mellom de behandlingsansvarlige. Ved skade som følge av overtredelse av personvernforordningen, skal hver behandlingsansvarlig holdes ansvarlig for hele skaden, med mulighet til å kreve regress, jf. personvernforordningen artikkel 82 nr. 4 og 5. Etter personvernforordningen artikkel 26 nr. 3 kan den registrerte utøve sine rettigheter overfor hver av de behandlingsansvarlige, uavhengig av den innbyrdes ansvarsfordelingen. Tilsynsmyndigheten vil også kunne forholde seg til alle de behandlingsansvarlige som kontaktpunkt, uavhengig av den interne ansvarsfordelingen. Dette er begrunnet i å sikre en effektiv håndhevelse av personvernregelverket.

2.2. NAV-loven

2.2.1 Generelt

Formålet med NAV-loven er å legge til rette for en effektiv arbeids- og velferdsforvaltning som er tilpasset den enkeltes og arbeidslivets behov, og som er basert på en helhetlig og samordnet gjennomføring av arbeidsmarkedsloven, folketrygdloven, lov om sosiale tjenester i arbeids- og velferdsforvaltningen og andre lover som forvaltes av arbeids- og velferdsforvaltningen. Dette framgår av NAV-lovens formålsparagraf (§ 1).

NAV-loven gir det formelle lovgrunnlaget for arbeids- og velferdsforvaltningen, herunder det rettslige rammeverket for det lokale samarbeidet som skal være mellom Arbeids- og velferdsetaten og kommunene. Arbeids- og velferdsetaten og kommunene skal ha felles lokale kontorer som dekker alle kommuner. NAV-kontoret skal ivareta oppgaver for Arbeids- og velferdsetaten *og* for kommunens oppgaver etter sosialtjenesteloven. Etaten og kommunene kan også avtale at andre av kommunens tjenester kan inngå i kontoret, jf. NAV-loven § 14 andre ledd.

Et av hovedmålene med NAV-reformen var å legge til rette for en mer helhetlig og samordnet arbeids- og velferdsforvaltning. Formålet var blant annet å få flere i arbeid, støtte opp under arbeidet med et inkluderende arbeidsliv og ivareta brukernes og arbeidslivets behov på en bedre måte.

Behandlingsansvaret for personopplysninger i arbeids- og velferdsforvaltningen har en begrenset omtale i NAV-loven. NAV-loven § 3 tredje ledd, andre punktum gir departementet hjemmel til å fastsette forskrift som nærmere regulerer behandlingsansvaret i arbeids- og velferdsforvaltningen.

I Ot.prp. nr. 47 (2005–2006) kapittel 12 merknad til § 3 tredje ledd første punktum, framgår det:

> «Tredje ledd første punktum legger ansvaret for oppfølging av forpliktelser etter personopplysningsloven til direktoratet når det gjelder Arbeids- og velferdsetaten. På kommunens område ligger dette til den enkelte kommunen og det forutsettes at samarbeidet reguleres i forbindelse med avtaleinngåelsen, jf. § 14 første ledd.

> I tredje ledd annet punktum gis departementet hjemmel til å gi forskrifter på området for hele arbeids- og velferdsforvaltningen. Dette kan være nødvendig og hensiktsmessig ved opplysninger som innhentes og brukes av både statsetaten og kommunesektoren, eventuelt også ved gjennomføringen av bestemmelsen i § 15 i lovforslaget om behovsavklaring og individuell plan.»

Det er per i dag ikke gitt forskrifter med hjemmel i NAV-loven § 3 tredje ledd.

Behandling av personopplysninger i forbindelse med NAV-loven § 14 a ble omtalt i Prop.135 L (2019–2020) Endringer i arbeids- og velferdsforvaltningsloven, sosialtjenesteloven, lov om Statens pensjonskasse og enkelte andre lover, punkt 6.1.2.4. Der står det:

> «Arbeids- og velferdsforvaltningsloven § 14 a synes forutsetningsvis å gi arbeids- og velferdsforvaltningen behandlingsgrunnlag for å innhente og behandle en rekke opplysninger knyttet til brukers situasjon. Bestemmelsen gir ingen spesifikk anvisning med hensyn til hvilke personopplysninger arbeids- og velferdsforvaltningen har rett til å innhente og til hvilket formål personopplysningene kan brukes.»

Dette lovforarbeidet hadde sin bakgrunn i at personvernforordningen ble innlemmet i EØS-avtalen. Behandling av personopplysninger på arbeids- og velferdsforvaltningens område er av et stort omfang, og opplysningene er ofte av sensitiv art. Opplysningene vil i tillegg ofte lagres over lengre tid. Dette gjør inngrepet i den enkeltes privatliv betydelig, noe som forsterker kravet til et tydelig fastsatt rettslig grunnlag. Departementet vurderer derfor at en uttrykkelig bestemmelse bedre vil være i samsvar med forordningens føringer om tydelighet og forutsigbarhet, jf. fortalepunkt 41.

2.2.2 NAV-loven § 14 a

NAV-loven § 14 a ble tilføyd ved lov 19. desember 2008, og trådte i kraft 1. februar 2010.

I tillegg til retten til å få en behovs- og arbeidsevnevurdering, regulerer bestemmelsen retten til å delta i utarbeidelsen av en konkret plan for hvordan brukeren skal komme i arbeid (aktivitetsplan).

Behovs- og arbeidsevnevurderingen er en vurdering av brukers ressurser og behov rettet mot arbeid, samt en vurdering av mulighetene i arbeidsmarkedet. Alle brukere som omfattes av bestemmelsen har rett til et vedtak om oppfølging (oppfølgingsvedtak). Oppfølgingsvedtaket skal beskrive brukerens nåsituasjon, hvilket mål brukeren har med tanke på arbeid og hvilke virkemidler som trengs for å nå målet, jf. første ledd bokstav a til e. Vedtaket er utgangspunktet for det videre oppfølgingsløpet, der andre tjenester vil være aktuelle. Det kan være både statlige og kommunale tjenester som tilbys av arbeids- og velferdsforvaltningen. Bestemmelsen skal bidra til at brukere med behov for hjelp til å komme i arbeid får en helhetlig vurdering. Vurderinger etter § 14 a er både en rettighet og tjeneste i seg selv, men samtidig et premiss og en forutsetning for en rekke etterfølgende avgjørelser av stor betydning for den enkelte bruker.

For å kunne foreta vurderinger etter § 14 a er det nødvendig å behandle personopplysninger. Personopplysninger innhentes blant annet gjennom registreringer i IT-

løsninger. IT-løsningene som benyttes, utvikles og forvaltes av Arbeids- og velferdsetaten, men både kommunalt og statlig ansatte på NAV-kontorene benytter disse. Tilgangen til opplysninger skal begrenses til ansatte på det enkelte kontor basert på tjenstlig behov.

3. Departementets vurderinger og forslag

3.1 Behovet for en forskrift om behandlingsansvar

Departementet vurderer at det ikke fremgår tydelig av gjeldende rett om det er statlig og/eller kommunal del av NAV-kontoret som er behandlingsansvarlig for innsamling og bruk av personopplysninger etter § 14 a. Dette medfører usikkerhet om hvilket ansvar de ulike aktørene som er involvert i behandlingen har, og utgjør dermed en risiko for at de registrertes rettigheter ikke blir tilstrekkelig ivaretatt.

NAV-loven § 14 a gir et rettslig grunnlag for å innhente og bruke personopplysninger knyttet til brukers situasjon. Omfanget av personopplysninger som behandles kan være stort, og kan omfatte særlige kategorier av personopplysninger (sensitive personopplysninger). Det tilsier at det ikke bør være uklarheter om hvem som har behandlingsansvaret for behandlingen av personopplysningene.

I punkt 2.1.1 er det vist til at forordningen artikkel 26 peker på ulike måter å fastlegge behandlingsansvar på. I denne saken mener departementet at det er mest hensiktsmessig å regulere behandlingsansvaret som følger av NAV-loven § 14 a i forskrift med hjemmel i NAV-loven § 3. Departementet mener det er nødvendig å tydeliggjøre hvem som har behandlingsansvaret, og at informasjon om dette er lett tilgjengelig både for arbeids- og velferdsforvaltningen og for de registrerte. Tydelighet, tilgjengelighet og forutsigbarhet er forhold som er vektlagt i departementets vurdering.

Alternativet til å regulere forholdet i forskrift er at ansvarsforholdene og spørsmål knyttet til dette reguleres gjennom enkeltstående avtaler mellom aktørene. Det ville i praksis bety avtaler mellom Arbeids- og velferdsetaten og landets per i dag 356 kommuner. Dette er etter departementets syn ikke en hensiktsmessig måte å regulere området på.

For det første er slike avtaler generelt ikke like tilgjengelig for de registrerte som forskrifter er. For det andre er et avtaleregime mellom direktoratet og hver av landets kommuner svært krevende, for alle parter. På den ene siden er det slik at for å sikre en enhetlig og gjennomførbar praksis, må innholdet i alle avtalene være likt. Det kan ikke være ulik praksis, ulike IT-systemer og ulike avtaler for gjennomføring av NAV-loven § 14 a ut over landet. På den andre siden vil et avtaleregime med over 350 avtaler og avtaleparter være svært omfattende og byrdefullt å administrere. Etter departementets syn er en slik omfattende administrasjon ikke hensiktsmessig bruk av fellesskapets ressurser, verken på statlig eller kommunal side. Det er blant annet ikke effektiv ressursbruk i landets kommuner at de må ta stilling til og forvalte avtaler med direktoratet som kommunene i svært liten grad kan påvirke innholdet i. Disse ressursene burde i stedet brukes til å yte primærtjenestene i NAV.

Departementets forslag til forskrift har til hensikt å uttømmende regulere behandlingsansvaret for behandling av personopplysninger ved vurdering av bistandsbehov

etter NAV-loven § 14 a. Det skal ikke være nødvendig med supplerende regulering mellom de behandlingsansvarlige. Departementet ber om høringsinstansenes innspill til om forslaget er dekkende for dette formålet, eller om det er flere forhold ved ansvarsfordelingen som bør reguleres.

3.2 Plassering av behandlingsansvaret

3.2.1 Hvem som er behandlingsansvarlig for personopplysninger etter NAV-loven § 14 a

NAV-loven § 14 a legger til grunn at NAV-kontoret skal ha en felles tilnærming og metodikk for å vurdere personers ressurser og bistandsbehov rettet mot arbeid, uavhengig om personen har behov for eller har søkt om kommunale eller statlige tjenester og ytelser. En felles tilnærming skal ivareta retten til en likeverdig og god vurdering for alle som henvender seg til NAV-kontoret. Metoden er en helhetlig kartlegging av sosiale forhold, arbeidserfaring, kompetanse, personlige egenskaper og eventuelle helseutfordringer i relasjon til arbeid. Avklaringen av hvilke tjenester og ytelser som anses som aktuelle for brukeren, skjer underveis i vurderingen. Det kan også være at vurderingen endres etter hvert som en person er under oppfølging fra NAV-kontoret.

NAV-loven § 14 a fjerde ledd første setning gir forvaltningsansvaret for at vurderingene blir gjennomført til Arbeids- og velferdsetaten: *«Arbeids- og velferdsetaten har ansvaret for at vurderingene blir gjennomført, og at aktivitetsplanene blir utarbeidet».* NAV-loven § 14 andre ledd åpner for at ansatte i stat og kommune i et NAV-kontor kan utføre oppgaver på hverandres myndighetsområder. Det innebærer at både statlig og kommunalt ansatte kan gjøre vurderinger etter § 14 a. Det praktiseres noe ulikt mellom NAV-kontorer om det er både statlig eller kommunalt ansatte som faktisk gjør vurderinger etter § 14 a. Personopplysninger som behandles, registreres i en felles IT-løsning som både statlige og kommunalt ansatte har tilgang til.

Resultatet av vurderinger etter NAV-loven § 14 a er en forutsetning for at andre oppgaver kan iverksettes, både kommunale og statlige oppgaver. Rett til kvalifiseringsprogram (KVP) etter sosialtjenesteloven § 29 forutsetter for eksempel at søkeren har gjennomgått en arbeidsevnevurdering og at tett og koordinert bistand gjennom deltakelse i programmet vurderes som hensiktsmessig og nødvendig for å styrke mulighetene i arbeidslivet. For kommunene vil et av formålene med behandlingen av opplysninger etter § 14 a være å ivareta sitt ansvar knyttet til kvalifiseringsprogrammet. For Arbeids- og velferdsetaten er behandling av personopplysninger etter § 14 a essensielt for flere statlige oppgaver, som å vurdere deltakelse i arbeidsmarkedstiltak og ulike ytelser etter folketrygdloven, som retten til arbeidsavklaringspenger (AAP) og uføretrygd. Koblingen mellom behovs- og arbeidsevnevurderinger og andre tjenester og ytelser er ønsket og nevnt i forarbeidene til de relevante bestemmelsene.

Departementet har vurdert mulige konsekvenser av ulik plassering av behandlingsansvaret for behandling av personopplysninger etter NAV-loven § 14 a (se 2.1.1 om ulike måter å fastlegge behandlingsansvar på). Om behandlingsansvaret legges til én av partene, vurderer vi at det kan medføre risiko for at personopplysningene som behandles ikke kan benyttes

for å ivareta både kommunens og statens oppgaver i et eventuelt videre oppfølgingsløp. Det vil ikke være i samsvar med intensjonen i § 14 a i NAV-loven. En annen tilnærming er å anse kommunen og Arbeids- og velferdsetaten som selvstendige behandlingsansvarlige for hver sine behandlinger. På tidspunktet når personopplysningene samles inn og vurderingen gjøres, er det ikke bestemt hvorvidt tiltak, tjenester og ytelser er statlige og /eller kommunale. Dette kan også endre seg underveis i § 14 a-vurderingen. Departementet vurderer at det vil være svært vanskelig å praktisere selvstendig behandlingsansvar for ulike deler av behandlingen på en enkel og tydelig måte. Når ansvarsforholdet mellom aktører som er involvert i behandlingen er uklar, kan det føre til at personvernet svekkes.

For å sikre at vurderinger som gjøres og personopplysningene som behandles ivaretar hele arbeids- og velferdsforvaltningen i henhold til intensjonen med § 14 a i NAV-loven, og at ansvarsforholdet mellom de to aktørene er tydelig, anser departementet at Arbeids- og velferdsetaten og kommunene er felles behandlingsansvarlige for personopplysninger som behandles etter NAV-loven § 14 a. Vi vurderer at felles behandlingsansvar samlet sett er den løsningen som innebærer minst utfordringer, og har i liten grad identifisert praktiske utfordringer som utelukkende inntrer ved felles behandlingsansvar. I vurderingen legger departementet også vekt på hvordan behandlingsansvaret er omtalt i Prop.135 L (2019–2020) *Endringer i arbeids- og velferdsforvaltningsloven, sosialtjenesteloven, lov om Statens pensjonskasse og enkelte andre lover punkt 6.1.2.4* (se omtale i 2.2.1), som Stortinget har sluttet seg til. I denne lovproposisjonen pekes det på at NAV-loven § 14 a forutsetningsvis gir *arbeids- og velferdsforvaltningen* behandlingsgrunnlag for å innhente og behandle en rekke opplysninger knyttet til brukers situasjon. Det gir støtte til vurderingen om at behandlingsansvaret ligger til arbeids- og velferdsforvaltningen.

Departementet foreslår at felles behandlingsansvar forskriftsfestes i § 3 i en ny forskrift om behandlingsansvar for behandling av personopplysninger i arbeids- og velferdsforvaltningen etter NAV-loven § 14 a.

3.3 Felles behandlingsansvar, ulik oppgave- og ansvarsfordeling

3.3.1 Felles behandlingsansvar og oppgave- og ansvarsfordeling mellom de behandlingsansvarlige

Felles behandlingsansvar er regulert av personvernforordningen artikkel 26. Departementet foreslår at det i § 3 i den nye forskriften eksplisitt vises til denne artikkelen.

Et felles behandlingsansvar innebærer at partene i felleskap er ansvarlige for at behandlingen av personopplysninger skjer i overensstemmelse med personvernforordningen, se punkt 2.1.2. Arbeids- og velferdsetaten og den enkelte kommune er som felles behandlingsansvarlige eksternt solidarisk ansvarlig overfor de registrerte og Datatilsynet. De registrerte og tilsynsmyndigheten kan henvende seg til én av de to behandlingsansvarlige.

Et felles behandlingsansvar vil ikke føre til mer ustrakt behandling eller utveksling av personopplysninger mellom Arbeids- og velferdsetaten og den enkelte kommune, eller mellom kommuner. Behandlingen begrenses av formålet og behandlingsgrunnlaget, og det

innebærer at behandlingen begrenses til personopplysninger som skjer med hjemmel i NAV-loven § 14 a.

Et felles behandlingsansvar mellom Arbeids- og velferdsetaten og kommunene betyr ikke at oppgaver og ansvar er likt fordelt mellom partene. Tvert imot anser departementet at et likt fordelt ansvar verken er realistisk eller hensiktsmessig. Departementet understreker at det ikke er noen motsetning mellom å være felles behandlingsansvarlige, og å ha en ulik innbyrdes ansvarsfordeling mellom de behandlingsansvarlige, se punkt 2.1.2.

Et felles behandlingsansvar innebærer videre ikke at Arbeids- og velferdsetaten eller den enkelte kommune er ansvarlig for forutgående eller etterfølgende behandling som den andre parten er ansvarlig for alene. Dette gjelder for eksempel for behandling av personopplysninger som ikke er direkte hjemlet i NAV-loven § 14 a. Forskriftens virkeområde avgrenses til å gjelde behandlinger etter § 14 a.

3.3.2 Kontaktpunkt for de registrerte

Når Arbeids- og velferdsetaten og den enkelte kommune er felles behandlingsansvarlige, innebærer det at begge parter er et kontaktpunkt mot den registrerte. Den registrerte skal få oppfylt sine rettigheter der personen henvender seg.

At den registrerte kan forholde seg til den behandlingsansvarlige personen ønsker, følger av kravene til den behandlingsansvarlige i personvernforordningen kapittel III. Departementet mener at det likevel vil være hensiktsmessig at det også framgår tydelig av forskriften som foreslås i dette høringsnotatet. Departementet foreslår at det framgår av § 5 første ledd i forskriften. Det skaper forutsigbarhet og avklaring både for den registrerte og de behandlingsansvarlige imellom.

At begge behandlingsansvarlige også er likeverdige kontaktpunkter mot tilsynsmyndigheten, det vil si Datatilsynet, er etter departementets syn ikke nødvendig å regulere særskilt i forskriften. Regelen følger av forslaget til § 3, og det vurderes at det ikke er samme behov for presisering blant profesjonelle aktører som overfor privatpersoner.

3.4 De behandlingsansvarliges ansvar for etterlevelse i egen virksomhet

3.4.1 Ansvar for etterlevelse i egen virksomhet

I Arbeids- og velferdsetaten er det Arbeids- og velferdsdirektoratet som er behandlingsansvarlig for etatens behandling av personopplysninger. Dette framgår av NAV-loven § 3 siste ledd første setning. Hvem som er behandlingsansvarlig i den enkelte kommune, fastsettes av kommunen selv utfra gjeldende regler for fastsettelse av behandlingsansvar.

De behandlingsansvarlige har det overordnede ansvaret for at krav i personvernregelverket (personopplysningsloven og personvernforordningen) etterleves. De behandlingsansvarlige, det vil si direktoratet og den enkelte kommune, må derfor sikre at behandlingsansvaret er ivaretatt innenfor egen virksomhet.

For tydelig å vise at den enkelte behandlingsansvarlige har ansvar for etterlevelse i egen virksomhet, foreslår departementet at dette forskriftsfestes i § 4 første ledd i forskriften. Ansvar for etterlevelse av kravene i forskriften foreslås fastsatt i samme bestemmelse.

I punkt 3.5.1 nedenfor og forslag til § 6 i forskriften foreslår departementet at Arbeids- og velferdsdirektoratet skal ha ansvar for personvern i IT-løsningen som benyttes i behandlingene. Det innebærer at kommunene ikke har ansvar for personvern knyttet til utvikling og forvaltning av selve IT-løsningene. Derimot har de ansvar for at bruken av IT-løsningene som skjer innenfor deres egen virksomhet bidrar til å overholde nødvendig sikkerhet for behandlingene. Kommunen har, på tilsvarende måte som Arbeids- og velferdsdirektoratet, blant annet ansvar for at rutiner for bruk av IT-løsningene følges innenfor egen virksomhet, slik det framgår av forslag til § 4 første ledd, der det slås fast at de behandlingsansvarlige hver for seg har ansvar for å etterleve kravene til behandling av personopplysninger i egen virksomhet. Se mer om rutiner i punkt 3.3.2 nedenfor. Videre har både direktoratet og den enkelte kommune ansvar for sikkerheten for behandlingene utenfor IT-løsningene i egen virksomhet.

3.4.2 Informasjonsdeling mellom de behandlingsansvarlige

For å kunne sikre etterlevelse i egen virksomhet trenger hver av partene informasjon om den andre partens virksomhet og behandling. Uten slik informasjon er det vanskelig å oppfylle ansvaret for etterlevelse i egen virksomhet.

For å sikre tilgang til den informasjonen som er nødvendig for å ivareta den enkeltes ansvar, foreslår departementet å forskriftsfeste en gjensidig informasjonsplikt mellom virksomhetene i § 4 andre ledd.

Departementet mener det ikke er hensiktsmessig å detaljregulere hvordan denne informasjonsutvekslingen skal foregå, verken med tanke på utvekslingsmetode, frekvens eller omfang. Dette bør etter departementets syn praktiseres i tråd med formålet med kravet og være en dynamisk standard som kan utvikle seg sammen med faktiske omstendigheter og teknologisk utvikling.

Departementet understreker at det er informasjon knyttet til behandlingen av personopplysningene og behandlingsansvaret som er relevant for informasjonsplikten som foreslås i forskriften. Utveksling av informasjon og konkrete personopplysninger er ikke ment regulert i denne forskriften. Dette reguleres gjennom andre regler, blant annet om taushetsplikt mv. I praksis vil det være informasjon om forhold i IT-løsningene som dekkes av forslaget til informasjonsplikt i § 4 andre ledd. Kommunene trenger for eksempel informasjon om direktoratets personvernkonsekvensvurderinger og sikkerhet i IT-løsningene for at kommunene skal kunne ivareta sitt ansvar som behandlingsansvarlig og blant annet føre egen protokoll over behandlinger.

3.5 Arbeids- og velferdsdirektoratets ansvar

3.5.1 Ansvar for IT-løsningene

Arbeids- og velferdsdirektoratet eier og har ansvar for IT-løsningene som brukes til behandlingen av personopplysninger som skjer med hjemmel i NAV-loven § 14 a. Departementet mener det både er rimelig og hensiktsmessig at ansvar for personvern og sikkerheten for behandlingene i disse IT-løsningene ligger til direktoratet. Selv om ansvaret som behandlingsansvarlig eksternt er felles og solidarisk, bør ansvaret for IT-løsningene legges til Arbeids- og velferdsdirektoratet. Ansvaret for IT-løsningene omfatter både utvikling og forvaltning av løsningene.

Departementet foreslår å regulere dette i forskriften § 6 første ledd.

Det innebærer at Arbeids- og velferdsdirektoratet i sin utvikling og forvaltning av IT-løsningene skal ivareta alle forpliktelsene som ligger til behandlingsansvarlig etter personvernforordningen. Arbeids- og velferdsdirektoratet skal dermed

- vurdere personvernkonsekvenser av behandlingene, jf. personvernforordningen artikkel 35
- sikre tilstrekkelig sikkerhetsnivå, jf. personvernforordningen artikkel 32
- ivareta kravene til innebygd personvern og personvern som standardinnstilling, jf. personvernforordningen artikkel 25
- sikre at løsningene er tilrettelagt for at de registrertes rettigheter kan bli oppfylt, jf. personvernforordningen kapittel III
- gi informasjon til de registrerte om hvordan personopplysningene behandles, jf. personvernforordningen artikkel 13

I forslag til § 4 andre ledd første setning er det foreslått en informasjonsplikt som skal sørge for nødvendig informasjonsutveksling mellom de behandlingsansvarlige. Plikten omfatter også informasjon om sikkerheten i IT-løsningene som brukes til behandling av personopplysninger som skjer med hjemmel i NAV-loven § 14 a. Det å forskriftsfeste direktoratets ansvar for IT-løsningene og informasjon til kommunene, vil etter departementets syn gi forutsigbarhet om hvilke plikter som ligger til de behandlingsansvarlige og hva de kan forvente av den andre aktøren. Det kan også styrke sikkerheten i IT-løsningene at ansvaret er tydelig plassert hos én aktør.

Departementet understreker at ansvarsreguleringen som foreslås i forskriften ikke endrer det økonomiske ansvaret for utvikling og forvaltning av IT-løsningene i arbeids- og velferdsforvaltningen.

3.5.2 Ansvar for rutiner

For å sikre at personvernet ivaretas i bruken av IT-løsningene, mener departementet at det må utarbeides nødvendige rutiner for dette. Utarbeidelse av rutiner henger nært sammen med ansvaret for personvern i utviklingen og forvaltningen av løsningene. Departementet foreslår derfor at Arbeids- og velferdsdirektoratet har ansvaret for dette. Å utarbeide tilpassede og hensiktsmessige rutiner forutsetter også god kjennskap til andre IT-løsninger

som brukes ved NAV-kontorene. Departementet foreslår at en plikt til å utarbeide rutiner for bruk av IT-løsningene tas inn i forskriften § 6 siste ledd.

Departementet mener også at det er hensiktsmessig at direktoratet, der det er behov, har plikt til å utarbeide rutiner for å ivareta de registrertes rettigheter for behandling av personopplysninger som behandles etter NAV-loven § 14 a. Departementet foreslår at dette tas inn i forskriften § 5 siste ledd. Ved å legge denne oppgaven til direktoratet gis det en tydelig oppgaveplassering, og sikres at det finnes felles rutiner som alle aktører benytter. Dette påvirker ikke hver av de behandlingsansvarliges ansvar for hvordan regelverket og rutinene følges og etterleves innenfor egen virksomhet. For å understøtte dette, foreslår departementet at dette presiseres i forskriften § 6 fjerde ledd siste punktum og § 5 andre ledd siste punktum.

3.6 Bruk av databehandlere

3.6.1 Mulighet til å bruke databehandlere

De behandlingsansvarlige kan bruke databehandlere i forbindelse med behandlingen av personopplysninger. Databehandlere vil da behandle personopplysninger på vegne av den behandlingsansvarlige.

I forbindelse med utførelse av NAV-loven § 14 a vil bruk av databehandlere være mest aktuelt for Arbeids- og velferdsdirektoratet som ansvarlig for IT-løsningene som brukes. Et praktisk eksempel kan være at Arbeids- og velferdsdirektoratet vil bruke eksterne skytjenester som en del av IT-løsningene. Retten til å overlate behandlingen av personopplysninger til databehandlere, og forpliktelsene som må være overholdt, gjelder imidlertid både for Arbeids- og velferdsetaten og den enkelte kommune.

3.6.2 Minimumskrav til den som vil bruke databehandler

Den behandlingsansvarlige er ansvarlig for databehandlerens etterlevelse av personvernregelverket. Relasjonen mellom den behandlingsansvarlige og databehandleren er regulert gjennom personvernforordningen artikkel 28 og 29. Relasjonen er derfor ikke nødvendig å regulere i forskriften som departementet foreslår i dette høringsnotatet. Departementet vil likevel peke på noen forhold som den behandlingsansvarlige som overlater behandlingen av personopplysninger til en databehandler må sørge for:

- Den behandlingsansvarlige som overlater behandling til en databehandler, skal vurdere om databehandleren er kompetent til å behandle personopplysningene i samsvar med personopplysningsloven. Det er flere krav som må vurderes i denne sammenheng. Bare hvis databehandleren er kompetent, er det tillatt å gå videre og bruke virksomheten som databehandler.
- Det må inngås en avtale med databehandleren som oppfyller kravene i personvernforordningen artikkel 28 nr. 3.
- Den behandlingsansvarlige som benytter en databehandler, skal informere den andre behandlingsansvarlige om avtalen som er inngått. Dette er en del av informasjonsplikten foreslått i § 3 andre ledd.

Departementet understreker at disse tre framhevede kravene er overordnede minimumskrav, og at de verken er uttømmende eller til erstatning for andre krav etter personvernregelverket som gjelder for de behandlingsansvarlige.

De behandlingsansvarlige kan ikke sette ut (outsource) ansvaret for å oppfylle forpliktelsene i personvernregelverket og forskriften.

3.7 Avvik og håndtering av brudd på sikkerheten ved behandlingen av personopplysninger

3.7.1 Hvem skal ha ansvar for håndtering av brudd på sikkerheten ved behandlingen

Det vil være en kritisk situasjon hvis det oppstår brudd på personopplysningssikkerheten. Det kan innebære brudd på konfidensialitet, integritet eller tilgjengelighet. Slike brudd kan skje hos begge de behandlingsansvarlige. Likevel vil det ofte kunne ha størst konsekvenser hvis det skjer i IT-løsningene.

Ansvaret for brudd på sikkerheten følger av personvernforordningen artikkel 32 til 34. Departementet har vurdert om det er hensiktsmessig også å fastsette ansvaret i den nye forskriften. Begrunnelsen kunne være å skape klarhet om ansvarsforholdet ettersom dette er særlig viktig i forbindelse med sikkerhetsbrudd. I slike situasjoner er det avgjørende at det ikke oppstår passivitet eller utydelighet om hvem som har ansvaret og hva som skal gjøres for å rette opp avviket. Departementet mener imidlertid at å presisere forpliktelser som allerede følger av personvernforordningen kan øke risikoen for at det oppstår utilsiktede avvik mellom forordning og sektorregulering. For å unngå dette, foreslår departementet ikke å presisere det i forskriftsteksten.

Departementet mener det er rimelig og hensiktsmessig at ansvaret for håndtering av brudd på sikkerheten ved behandlingen som hovedregel ligger på Arbeids- og velferdsdirektoraret. Det er etter departementets syn en naturlig forlengelse av at direktoratet også har ansvar for IT-løsningene, se forslag til § 6.

Samtidig kan det være tilfeller der bruddet ikke er knyttet til IT-løsningene, men derimot knyttet til forhold som helt og holdent er innenfor en kommunes kontrollsfære. Eksempler på dette kan være at en kommunalt ansatt ved et NAV-kontor gjør et sikkerhetsbrudd, for eksempel legger igjen PC-en på bussen, lar være å sikkerhetsmakulere dokumenter med sensitiv informasjon e.l. I slike tilfeller er det verken rimelig eller nyttig at Arbeids- og velferdsdirektoratet har ansvaret for håndteringen av bruddet. Departementet har også lagt vekt på at det vil være unødig byrdefullt og omfattende for begge parter om kommunene skal involvere stat i «mindre og lokale» brudd. Hva som er helt og holdent innenfor kommunens sfære, må alltid vurderes konkret.

Departementet foreslår derfor et unntak fra hovedregelen knyttet til slike situasjoner, se forslag til § 8 første ledd andre setning. Departementet understreker at dette er et smalt unntak.

3.7.2 Varsel til den andre behandlingsansvarlige ved brudd på personopplysningssikkerheten

Ovenfor har departementet foreslått en gjensidig informasjonsplikt mellom de behandlingsansvarlige, jf. forslag til § 4 andre ledd første setning. At de andre behandlingsansvarlige skal ha informasjon om brudd på personopplysningssikkerheten følger denne regelen. Departementet anser likevel at det er hensiktsmessig å forskriftsfeste en særlig tydelig plikt til å varsle de andre behandlingsansvarlige ved brudd på personopplysningssikkerheten. Departementet foreslår at slike brudd skal varsles snarest mulig, jf. forslag til § 8 siste ledd. Siden behandlingsansvaret er felles, jf. forslag til § 3 i forskriften, er det viktig at de behandlingsansvarlige seg imellom har en tydelig oppgavefordeling og vet hva de kan holde hverandre ansvarlige for.

Som omtalt ovenfor vil det for de fleste tilfeller være Arbeids- og velferdsdirektoratet som er ansvarlig for håndtering av bruddet, og som også har plikt til å varsle de andre behandlingsansvarlige. Ofte vil det bety å varsle alle kommunene, ettersom alle kommuner vil påvirkes av brudd på sikkerheten som skjer i IT-løsningene.

Samtidig har departementet beskrevet at det kan være situasjoner der et brudd skjer helt og holdent innenfor en kommunes virksomhet og ansvar, og at kommunen derfor har ansvar for håndteringen av bruddet. I slike tilfeller vil kommunens varslingsplikt gjelde overfor de andre behandlingsansvarlige som er berørt. Dette vil som regel være direktoratet ettersom bruddet gjerne har skjedd på et NAV-kontor som drives i partnerskap. Det kan også være at andre kommuner er berørt hvis NAV-kontoret for eksempel drives som et samarbeid mellom flere kommuner.

Plikten til å varsle den andre behandlingsansvarlige ved brudd på personopplysningssikkerheten, påvirker ikke plikten til å håndtere bruddet, se forslag til § 8 første og andre ledd.

3.8 Oversikt over ansvar og oppgaver

Tabellen gir en oversikt over ansvars- og oppgavefordelingen mellom Arbeids- og velferdsetaten og kommunene:

Ansvaret til Arbeids- og velferdsetaten	**Ansvaret til kommunene**
Ansvar overfor de registrerte og tilsynsmyndigheten for at de behandlingsansvarliges forpliktelser overholdes (felles behandlingsansvar)	Ansvar overfor de registrerte og tilsynsmyndigheten for at de behandlingsansvarliges forpliktelser overholdes (felles behandlingsansvar)
Ansvar for utvikling og forvaltning av IT-løsningene	
Ansvar for å utarbeide nødvendige rutiner for å ivareta de registrertes rettigheter	
Ansvar for å utarbeide nødvendige rutiner for IT-løsningene	
Ansvar for at rutinene for å ivareta de registrertes rettigheter og for IT-	Ansvar for at rutinene for å ivareta de registrertes rettigheter og for IT-

løsningene følges innenfor egen virksomhet	løsningene følges innenfor egen virksomhet
Ansvar for å håndtere brudd på sikkerheten i behandlingen, inkludert å varsle kommunene • vurdere om det skal sendes melding til tilsynsmyndigheten • vurdere om registrerte som er berørt av bruddet skal underrettes	Ansvar for å håndtere brudd på sikkerheten som helt og holdent er innenfor en kommunes virksomhet og ansvar, inkludert å varsle de berørte behandlingsansvarlige • vurdere om det skal sendes melding til tilsynsmyndigheten • vurdere om registrerte som er berørt av bruddet skal underrettes
Ansvar for at egen virksomhet, herunder egne ansatte, følger kravene i personopplysningsloven og forskriften	Ansvar for at egen virksomhet, herunder egne ansatte, følger kravene i personopplysningsloven og forskriften
Ansvar for å gi den andre parten informasjon som er nødvendig for at den skal kunne oppfylle krav ihht. personopplysningsloven og forskriften	Ansvar for å gi den andre parten informasjon som er nødvendig for at den skal kunne oppfylle krav ihht. personopplysningsloven og forskriften
Ansvar for å ivareta rollens om kontaktpunkt for de registrerte	Ansvar for å ivareta rollens om kontaktpunkt for de registrerte

4. Økonomiske og administrative konsekvenser

Forslaget har til hensikt å tydeliggjøre det felles ansvaret for behandling av personopplysninger etter NAV-loven § 14 a. Forslagene innebærer ikke en endring av forvaltningsansvaret for verken stat eller kommune. Forslaget vil derav ikke ha økonomiske konsekvenser.

En tydeliggjøring av hvordan behandlingsansvaret er fordelt og hvilke aktiviteter som er knyttet til ansvaret, vil gjøre det enklere og mer forutsigbart for de ansvarlige å forholde seg til og etterleve regelverket. Forslaget innebærer etter departementets syn dermed en mindre administrativ forenkling.

5. Forslag til forskrift om behandlingsansvar for behandling av personopplysninger i arbeids- og velferdsforvaltningen etter NAV-loven § 14 a

Hjemmel: Lov om arbeids- og velferdsforvaltningen (NAV-loven) § 3 tredje ledd

§ 1 *Formål*

Forskriften skal legge til rette for at arbeids- og velferdsforvaltningen ivaretar de registrertes rett til vern om sine personopplysninger, og fastsetter hvem som har ansvaret for å gjennomføre tiltak som er nødvendige for å oppfylle forpliktelsene til behandlingsansvarlige.

§ 2 *Virkeområde*

Forskriften regulerer behandlingsansvaret i arbeids- og velferdsforvaltningen for behandling av personopplysninger ved vurdering av bistandsbehov etter NAV-loven § 14 a.

§ 3 *Felles behandlingsansvar*

Arbeids- og velferdsetaten og den enkelte kommune er felles behandlingsansvarlige, jf. personvernforordningen artikkel 26, for behandling av personopplysninger som skjer ved vurderinger etter NAV-loven § 14 a.

Ansvarsfordelingen mellom Arbeids- og velferdsetaten og den enkelte kommune følger av §§ 4, 5, 6 og 7.

§ 4 *Ansvaret til de behandlingsansvarlige*

Arbeids- og velferdsetaten og den enkelte kommune skal sørge for at kravene i lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) og i denne forskriften etterleves innenfor egen virksomhet. De behandlingsansvarlige skal, med utgangspunkt i sine forpliktelser, utarbeide nødvendige rutiner for å ivareta sine forpliktelser, og sørge for at rutinene følges i egen virksomhet.

Behandlingsansvarlige som overlater behandlingen til en databehandler, har ansvaret for at personvernregelverket og kravene i denne forskriften ivaretas, jf. personvernforordningen artikkel 4, 28 og 29.

Arbeids- og velferdsetaten og den enkelte kommune skal gi hverandre nødvendig informasjon for at den andre parten skal kunne oppfylle sine forpliktelser etter første ledd.

§ 5 *Ansvar for de registrertes rettigheter*

Arbeids- og velferdsetaten og den enkelte kommune er som felles behandlingsansvarlige begge kontaktpunkt for de registrerte, jf. personvernforordningen artikkel 26 (3).

Arbeids- og velferdsdirektoratet skal utarbeide nødvendige rutiner for å ivareta de registrertes rettigheter. Alle behandlingsansvarlige skal sørge for at rutinene følges i egen virksomhet.

§ 6 *Ansvar for personvern i IT-løsninger*

Arbeids- og velferdsdirektoratet har ansvar for at IT-løsningene som brukes til behandling av personopplysninger, oppfyller kravene i personvernregelverket herunder krav til sikkerhet ved behandlingen, jf. personvernforordningen artikkel 32. Ansvaret for IT-løsningene omfatter utvikling og forvaltning av løsningene.

Arbeids- og velferdsdirektoratet skal utarbeide nødvendige rutiner for bruk av IT-løsningene. De behandlingsansvarlige skal sørge for at rutinene følges innenfor egen virksomhet.

§ 7 *Håndtering av brudd på sikkerheten ved behandlingen*

Arbeids- og velferdsdirektoratet har ansvar for håndtering av brudd på sikkerheten ved behandlingen, inkludert i IT-løsningene. Håndteringen skal skje i samsvar med forpliktelsene etter personvernforordningen artikkel 33 og 34. Hvis bruddet helt og holdent er innenfor en kommunes virksomhet og ansvar, har kommunen likevel ansvar for håndtering av bruddet.

Ved brudd på personopplysningssikkerheten skal de andre berørte behandlingsansvarlige varsles snarest mulig.

§ 8 *Når forskriften trer i kraft*

Forskriften trer i kraft [dd.mm.åååå].

6. Merknader til bestemmelser i forskriften

Til § 1 Formålet med forskriften

Bestemmelsen regulerer formål med forskriften. Reglene i forskriften skal legge til rette for at de registrertes rettigheter til vern om sine personopplysninger ivaretas. Dette er konkretisert gjennom at forskriften gjelder plassering av ansvar for ulike oppgaver, aktiviteter og tiltak som de behandlingsansvarlige må gjennomføre for å ivareta sitt ansvar.

Hensikten med forskriften er å tydeliggjøre ansvarsforholdene, ikke å legge opp til mer utstrakt behandling eller utveksling av personopplysninger mellom Arbeids- og velferdsetaten og den enkelte kommune, eller mellom kommuner.

Formålet vil tjene som tolkningsstøtte for de øvrige bestemmelsene i forskriften.

Til § 2 Virkeområde

Det fastslås at det saklige virkeområdet for forskriften er behandling av personopplysninger som skjer for å gjennomføre aktivitetene i NAV-loven § 14 a. Avgrensingen av virkeområdet innebærer for det første at behandling av personopplysninger for andre formål enn dette ikke er dekket av forskriften. For det andre regulerer ikke forskriften andre plikter enn de som følger av personvernregelverket. Forpliktelser etter for eksempel arkivregelverket, forvaltningsrett mv. faller dermed utenfor.

Til § 3 Felles behandlingsansvar

Bestemmelsen regulerer behandlingsansvaret for behandling av personopplysninger som skjer med hjemmel i NAV-loven § 14 a.

I første ledd er det presisert at Arbeids- og velferdsetaten og den enkelte kommune er felles behandlingsansvarlige. Hensikten med å forskriftsfeste behandlingsansvaret er å skape klarhet, særlig for de registrerte. Felles behandlingsansvar skal tolkes og gjennomføres i samsvar med personvernforordningen artikkel 26.

At behandlingsansvaret er felles mellom Arbeids- og velferdsetaten og kommunene, betyr ikke at ansvaret er likt fordelt mellom partene. En ulik fordeling mellom partene er hensiktsmessig for å løse oppgavene knyttet til NAV-loven § 14 a mest mulig effektivt. Arbeids- og velferdsetaten og kommunene har i stor grad ulikt respektivt ansvar og hver sine oppgaver knyttet til behandlingene av personopplysninger som skjer når NAV-loven § 14 a skal oppfylles.

Andre ledd uttrykker at det er en ansvarsfordeling mellom Arbeids- og velferdsetaten og kommunene, og at ansvarsfordelingen følger av §§ 4, 5, 6 og 7.

Til § 4 Ansvaret til de behandlingsansvarlige

Første ledd presiserer at hver av de behandlingsansvarlige har ansvar for at deres egen virksomhet, herunder deres egne ansatte, etterlever kravene i personvernregelverket og forskriften. Dette ansvaret må de behandlingsansvarlige ivareta gjennom betryggende internkontroll og andre tiltak knyttet til å sikre etterlevelse. I praksis vil det være ulike oppgaver som er aktuelle hos de ulike behandlingsansvarlige. Dette følger både av aktivitetene knyttet til NAV-loven § 14 a og ansvars- og oppgavedelingen i forskriften §§ 4, 5, 6 og 7. Arbeids- og velferdsetaten og kommunene har ansvar for de aktivitetene som deres ansatte på NAV-kontorene gjennomfører.

I andre ledd er det understreket at behandlingsansvarlige som overlater behandlingen til en databehandler, likevel har ansvar for at krav i personvernregelverket og forskriften etterleves. For personvernregelverket følger det samme av personvernforordningen artikkel 28 mv. Ansvaret som behandlingsansvarlig endres ikke av at behandlingen overlates til databehandlere. I forbindelse med utførelse av NAV-loven § 14 a vil bruk av databehandlere være mest aktuelt for Arbeids- og velferdsdirektoratet som eier av IT-løsningene som brukes. Et praktisk eksempel på bruk av databehandlere kan være at Arbeids- og velferdsdirektoratet bruker eksterne skytjenester som en del av IT-løsningene.

Tredje ledd gir de behandlingsansvarlige en gjensidig plikt til å dele informasjon med hverandre. Hver av de behandlingsansvarlige plikter å gi den andre den informasjonen som er nødvendig for at den andre parten skal kunne oppfylle sine forpliktelser etter personvernregelverket og forskriften. Dette vil typisk være informasjon om forhold i IT-løsningene som brukes i forbindelse med NAV-loven § 14 a. Kommunene trenger blant annet informasjon om direktoratets personvernkonsekvensvurderinger og sikkerhet i IT-løsningene, for at de skal kunne ivareta sitt ansvar som behandlingsansvarlig, inkludert å føre sin egen protokoll over behandlinger. Informasjon om at behandlingen er overlatt til en databehandler, vil også være omfattet av informasjonsplikten.

Bestemmelsen innebærer ikke en detaljregulering av hvordan informasjonsutvekslingen skal foregå, verken med tanke på utvekslingsmetode, frekvens eller omfang. Dette må løses i tråd med formålet med kravet og være en dynamisk standard som kan utvikle seg sammen med faktiske omstendigheter og teknologisk utvikling.

Informasjonsplikten gjelder bare informasjon knyttet til behandlingen av personopplysningene og behandlingsansvaret. Utveksling av informasjon og opplysninger

om den enkelte bruker er for eksempel ikke omfattet av regelen. Slike forhold reguleres gjennom annet regelverk, blant annet regler om taushetsplikt mv.

Til § 5 Ansvar for de registrertes rettigheter

Bestemmelsens første ledd presiserer at begge behandlingsansvarlige er kontaktpunkt for de registrerte. Det betyr at de registrerte kan henvende seg til den behandlingsansvarlige de selv ønsker for å få oppfylt sine rettigheter. Dette er en presisering av det som følger av personvernregelverket.

I andre ledd plasseres ansvaret for å utarbeide nødvendige rutiner for å ivareta de registrertes rettigheter på Arbeids- og velferdsdirektoratet. Ansvaret er plassert til direktoratet ettersom oppfyllelsen av rettighetene i stor grad er knyttet til IT-løsningene. Det er for eksempel direktoratet som må håndtere krav om innsyn i personopplysningene som er behandlet i IT-løsningene, eller krav om retting eller sletting av slike opplysninger.

Andre ledd andre punktum pålegger alle behandlingsansvarlige å sørge for at rutinene følges innenfor egen virksomhet. Dette legger til rette for at rutinene følges i praksis og at man dermed oppnår hensikten med rutinene; at de registrertes rettigheter ivaretas.

Til § 6 Ansvar for personvern i IT-løsninger

Bestemmelsens første ledd plasserer ansvaret til Arbeids- og velferdsdirektoratet for personvern i IT-løsningene som brukes til behandlingene. Det er understreket at krav til sikkerheten etter personvernforordningen artikkel 32 må være oppfylt. Ansvaret for personvern i IT-løsninger er regulert særskilt ettersom en vesentlig del av behandlingene vil skje i slike løsninger. Arbeids- og velferdsdirektoratet utvikler og forvalter IT-løsningene, og ansvaret for personvern i løsningene ligger derfor på direktoratet.

Bestemmelsens andre ledd første setning fastsetter at Arbeids- og velferdsdirektoratet har ansvar for å utarbeide nødvendige rutiner knyttet til bruken av IT-løsningene. Rutinene vil blant annet styre hvordan veiledere ved NAV-kontorene bruker IT-løsningene. Enhetlige rutiner vil legge til rette for en enhetlig praktisering slik at alle de registrertes personvern blir ivaretatt på en god nok måte. Bestemmelsen gir ikke en plikt til å etablere rutiner om det materielle innholdet i hvordan NAV-loven § 14 a skal forstås og ivaretas.

For å oppnå den ønskede effekten av rutinene fastslår andre ledd siste setning at alle behandlingsansvarlige har ansvar for at rutinene følges innenfor egen virksomhet.

Hvem som har ansvaret ved et eventuelt brudd på sikkerheten, framgår av en egen bestemmelse, § 7.

Til § 7 Håndtering av brudd på sikkerheten

Bestemmelsens første ledd regulerer hvilken av de behandlingsansvarlige som har ansvaret for håndtering av sikkerhetsbrudd. Ansvaret for sikkerhet i IT-løsningene er regulert i § 6. Et sikkerhetsbrudd er brudd på konfidensialitet, integritet eller tilgjengelighet, alternativt en kombinasjon av de ulike kategoriene av brudd. Ansvaret ligger etter forskriften til Arbeids- og velferdsdirektoratet, med unntak av de bruddene som skjer utelukkende innenfor en

kommunes virksomhet og kontrollsfære. Det er understreket at håndteringen skal skje i samsvar med forpliktelsene etter personvernforordningen.

Bestemmelsens andre ledd innebærer at den behandlingsansvarlige som identifiserer et sikkerhetsbrudd har en plikt til å varsle de andre berørte behandlingsansvarlige om bruddet. Hvilke behandlingsansvarlige som skal varsles, må vurderes fra sak til sak basert på hvilke andre behandlingsansvarlige som trenger informasjon for å overholde sine forpliktelser. Typiske tilfeller der det ikke er nødvendig å varsle andre behandlingsansvarlige er der sikkerhetsbruddet utelukkende er innenfor en kommunes ansvarsområde. I de tilfellene vil det ofte ikke være nødvendig å varsle andre kommuner om bruddet.