Datatilsynet

Arbeids- og velferdsdirektoratet - Styringsenheten IKT
Postboks 5200 Nydalen
0426 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	12/00116-8/CBR	24. september 2012

Vedtak om pålegg - endelig kontrollrapport for NAV Kontroll

Den 7. mars 2012 gjennomførte Datatilsynet en kontroll hos Arbeids- og velferdsdirektoratet, NAV Kontroll. Kontrollen fant sted med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 42 tredje ledd nr. 3.

Formålet med kontrollen var å belyse hvorvidt den behandling av personopplysninger som skjer i forbindelse med NAVs kontrollvirksomhet er i overensstemmelse med kravene i personopplysningsloven.

Tilsynet ønsket særlig å belyse hvorvidt kontrollvirksomheten gjennomføres i overensstemmelse med de fullmakter som er gitt av Stortinget gjennom folketrygdloven, og hvorvidt de registrerte får tilfredsstillende informasjon om den behandlingen som skjer. Tilsynet har også sett nærmere på om personopplysningslovens krav til internkontroll og informasjonssikkerhet er tilfredsstillende ivaretatt i enheten.

Datatilsynet utarbeidet en foreløpig kontrollrapport og oversendte varsel om vedtak den 22. mai 2012. Tilsynet mottok direktoratets tilsvar den 13. juni 2012, og har utarbeidet endelig utarbeidet en endelig kontrollrapport (vedlagt).

Faktagrunnlaget i kontrollrapporten er endret noe, i forhold til foreløpig rapport, i tråd med merknadene i direktoratets tilsvar. Endringene er imidlertid uten betydning for tilsynets vurderinger og de konklusjoner som ligger til grunn for dets varsel om vedtak.

I sitt tilsvar gjør NAV også rede for sine vurderinger av *de rettslige spørsmålene* som reises. Direktoratet tar i det vesentlige Datatilsynets vurderinger til etterretning, og har utarbeidet en plan for å etterleve det varslede vedtaket. Det forutsettes at NAV legger til grunn tilsynets vurderinger av hvilke plikter etaten har i henhold til personopplysningsloven når rutinene skal gjennomgås. Datatilsynet har forholdt seg til direktoratets tidsplan ved utforming av foreliggende vedtak, jf nedenfor

På ett område fremgår det uttrykkelig at NAV er uenige i tilsynets vurderinger av de rettslige forholdene, nemlig spørsmålet om rekkevidden av NAVs *informasjonsplikt* (pålegg 2). Direktoratets anførsler er behandlet særskilt nedenfor, under punktet "Kort om funn"

Kort om funn

Datatilsynets kontrollrapport viser at NAVs kontrollvirksomhet medfører en utstrakt og omfattende innhenting og videre behandling av personopplysninger, herunder av sensitiv karakter. Opplysningene kan knyttes både til stønadsmottakere og andre, og de hentes inn fra en stor krets personer, offentlige etater og virksomheter. Kontrollvirksomheten har til formål å avdekke hvorvidt det foreligger brudd på et regelverk som er straffesanksjonert. Informasjonsbehandlingen beror naturlig nok ikke på den enkeltes samtykke, men gjennomføres med hjemmel i lov.

Datatilsynet har avdekket betydelige mangler ved NAVs etterlevelse av personopplysningsregelverket i forbindelse med kontrollvirksomheten. Manglene er av en slik art at det kan stilles spørsmål ved om staten tilfredsstillende ivaretar rettssikkerheten til de personer som underlegges NAVs kontroll.

Krav om rettslig grunnlag - legalitetskontroll

I henhold til personopplysningslovens § 11 litra a er det forbudt å behandle personopplysninger uten at det foreligger et rettslig grunnlag etter personopplysningslovens § 8. Dersom det behandles personopplysninger som er sensitive kommer også de strengere vilkårene i personopplysningslovens § 9 til anvendelse. I forbindelse med NAVs kontrollvirksomhet behandles det sensitive personopplysninger blant annet i form av helseopplysninger.

Datatilsynet er av den oppfatning at NAVs behandling av personopplysninger i forbindelse med kontrollvirksomhet må ha *hjemmel i lov*, jf personopplysningslovens § 8 og 9.

Et klart lovverk er nødvendig for å sikre

- at forholdsmessigheten[1] i de kontrolltiltakene som iverksettes er belyst og vurdert i en demokratisk prosess,
- at den enkelte borger kan overskue hvorvidt og på hvilke vilkår hans forhold blir gjenstand for en kontroll, og
- at den enkelte borger forstår hvilke rettigheter og plikter han har i forbindelse med en kontroll.

NAVs kontrollvirksomhet[2] reguleres i hovedsak gjennom folketrygdloven. Denne gir i seg selv liten veiledning i hvordan NAV skal gjennomføre sine kontroller, med hensyn til innhenting og behandling av personopplysninger. I stor grad overlates dette til forvaltningens skjønn.

[1] Jf EMK art 8
[2] folketrygdlovens § 21-4 og 21-4a

Når folketrygdloven ikke angir konkrete rammer for kontrollvirksomheten blir det nærmest umulig også for Datatilsynet å vurdere hvorvidt NAV i praksis gjennomfører sine kontroller i overensstemmelse denne lovens med vilkår. Tilsynet har derfor ikke konkludert vedrørende dette.

Uklart regelverk, mangelfulle interne rutiner[3] og mulige mangler ved etterlevelsen av forvaltningsloven medfører imidlertid en klar risiko for at den behandling som skjer i det enkelte tilfellet ikke er i overensstemmelse med nasjonal lovgivning eller internasjonale forpliktelser.

Datatilsynet vil anbefale lovgiver enten å endre folketrygdlovens bestemmelser, eller i det minste å påse at det etableres et forskriftsverk som nærmere angir rammene for NAV i kontrolløyemed, herunder behandling av personopplysninger. Datatilsynet vil også sende en kopi av foreliggende varsel og foreløpige kontrollrapport til Sivilombudsmannen, for eventuell oppfølgning.

Informasjonsplikt

I henhold til personopplysningslovens §§ 19 og 20 skal den registrerte som hovedregel gis informasjon om behandling av personopplysninger. Informasjon er en grunnleggende rettighet som er nødvendig for at den registrerte skal kunne ivareta egne interessert som registrert ved behandlingen, for eksempel be om innsyn i de opplysningene som behandles eller få anledning til å supplere eller rette opplysningene.

Datatilsynet har avdekket at NAV som den klare hovedregel unnlater å informere den registrerte om sin innhenting og videre behandling av personopplysninger. Dette gjelder både de personer som kontrollen retter seg direkte mot, og andre registrerte. Tilsynet er ikke enig i NAV sine vurderinger av hvordan personopplysningslovens unntak fra informasjonsplikten skal forstås, og mener at NAV gir dem for vid anvendelse.

I sitt tilsvar av viser NAV til at de informerer i henhold til *forvaltningslovens* bestemmelser, ved at parten sendes varsel om vedtak. Datatilsynet vil bemerke at informasjonsplikten etter personopplysningsloven går videre enn varslingsbestemmelsen etter forvaltningsloven. Personkretsen etter forvaltningsloven gjelder for eksempel bare overfor parten, mens informasjonsplikten etter personopplysningsloven gjelder overfor alle de registrerte. I tillegg oppstår informasjonsplikten etter personopplysningsloven normalt tidligere enn varslingsplikten etter forvaltningsloven. Endelig er pliktens innhold ulikt. Mens det etter personopplysningsloven minst skal gis informasjonselementer som opplistet i § 19, skal parten etter forvaltningsloven varsles om innholdet i og saksgangen rundt et mulig enkeltvedtak. Det blir ikke gitt varsel i de tilfeller hvor kontrollhandlingene ikke leder til en etterfølgende forvaltningssak.

[3] Datatilsynet fant at det ikke var etablert interne rutiner i enheten for å sikre at folketrygdlovens vilkår er forsvarlig vurdert og oppfylt i det enkelte tilfellet. Datatilsynet mener at dette representerer et brudd på den internkontrollplikten som påhviler NAV i medhold av personopplysningslovens § 14, og det vises til vedtakets pkt 3

I sin ytterste konsekvens innebærer NAV sin praksis at personer som er eller har vært underlagt en kontroll aldri blir informert om hvilke behandlinger som har funnet sted. For eksempel om at NAV har vært i kontakt med den barnehagen hvor den kontrollerte har sine barn, hans arbeidsgiver, formannen i borettslaget hans og fra hans Facebook-vegg. I de tilfeller hvor en innhenting medfører at opplysninger om kontrollen blir kjent for personer i den kontrollertes omkrets er det særlig viktig med informasjon, for at den kontrollerte skal kunne avverge eller gis mulighet til å forholde seg til eventuelle rykter og spekulasjoner i nærmiljøet.

Datatilsynet ser svært alvorlig på denne praksisen, særlig hva gjelder informasjon til den som kontrollen direkte retter seg mot (typisk stønadsmottaker selv). I en kontrollsituasjon er kontradiksjonshensynet særlig viktig. Det vises til at opplysningene som hentes inn brukes til å treffe avgjørelser som er av stor betydning for den enkelte - ikke bare hva gjelder selve stønadsspørsmålet, men også i vurdering av ytterligere kontrolltiltak mot vedkommende og eventuell anmeldelse til politiet.

I sitt tilsvar anfører NAV at unntaket i personopplysningslovens § 20 annet ledd kommer til anvendelse på deres innhenting av personopplysninger i forbindelse med kontroller, idet behandlingen er uttrykkelig hjemlet i lov. Datatilsynet bestrider ikke at unntaket i prinsippet kan komme til anvendelse for NAV, og er således enig i Justisdepartementets vurderinger knyttet til dette[4]. Bestemmelsen kan imidlertid ikke forstås slik at enhver kontrollhandling som skjer med hjemmel i folketrygdlovens §§ 21-4 og 21-4a er unntatt. Det vises til at lovgiver eksplisitt har forutsatt at informasjonsplikten i personopplysningsloven skal ivaretas, til tross for at det foreligger en lovhjemmel. Datatilsynet mener at dette tilsier en forsiktig bruk av unntaket, og forutsetter NAV tar høyde for det når rutinene skal revideres. Datatilsynets rapport er derfor uendret på dette punktet.

Datatilsynet vil i denne forbindelse også bemerke at det klart gikk fram av NAVs rutiner at formålet med å unnlate informasjon uansett var "å unngå bevisforspillelse". Tilsynet kan ikke se at NAV har hatt merknader til foreløpig kontrollrapport, hva gjelder tilsynets vurderinger av vilkårene for bruk av dette unntaket. Punktet er derfor uendret i forhold til den foreløpige kontrollrapporten.

I sitt tilsvar til varsel om vedtak anfører NAV at etaten ikke vil ta opp avsluttede kontrollsaker for å informere de kontrollere, jf tilsynets varsel om vedtak pkt 4. NAV skriver i den forbindelse at det "ikke ser grunn" til å ta opp igjen gamle saker og foreta en fornyet gjennomgang av om vilkårene for informasjonsplikt foreligger.

Datatilsynet vil bemerke at pålegget er gitt med bakgrunn i at NAV mangler rutiner for å sikre at informasjonsplikten i ethvert tilfelle blir vurdert konkret og forsvarlig. Tilsynet har samtidig konkludert med at NAV gir unntakene fra informasjonsplikten for vid anvendelse, jf over. Det er derfor sannsynlig at NAV har unnlatt å gi informasjon i tilfeller hvor lovens unntak ikke kommer til anvendelse. Tilsynet vil videre bemerke at informasjonsplikten ikke faller bort som følge av manglende vurdering, eller en feilvurdering. Det er heller ikke slik at

[4] Lovavdelingens brev av 31. mai 2012.

retten til informasjon foreldes. Datatilsynet fastholder derfor sine vurderinger, og fatter vedtak i tråd med det som er varslet. Det er naturlig at gjennomgangen gjøres i tid etter at NAV har revidert sine rutiner for informasjonsplikt.

Sletting

Datatilsynet konstaterer at NAV kontroll mangler rutiner for oppbevaring og kassasjon som tilfredsstiller kravene i henholdsvis arkivloven og personopplysningsloven. Tilsynet legger til grunn at NAV vil oppfylle Riksarkivets pålegg, og for fremtiden vil etterleve arkivlovens bestemmelser.

Tilsynet legger videre til grunn at NAV samtidig etablerer *rutiner for å slette* de opplysningene som ikke skal arkiveres i henhold til arkivlov, eller oppbevares i medhold av annen lovgivning.

Informasjonssikkerhet

Datatilsynet har vurdert informasjonssikkerheten ved NAV Kontroll i henhold til kravene i personopplysningslovens § 13, jf. personopplysningsforskriftens kapittel 2. Tilsynet har lagt til grunn at NAV Kontroll gjennomgående behandler sensitive personopplysninger og at sikkerheten må avpasses deretter. Tipsbasen i Access har, slik NAV Kontroll har implementert løsningen, ikke tilfredsstillende informasjonssikkerhet. Spesielt er tilgangsstyringen for vid, da autentisering og autorisering ved pålogging skjer per avdeling og ikke per person. For elektroniske mapper er det ingen autentisering eller autorisering, annet enn generell tilgang til mapper på fellesområdet for avdelingen. Datatilsynet konkluderer med at bruken av Access og elektroniske filmapper ikke er i tråd med personopplysningsforskriften §§ 2-7 og 2-8, 3. ledd

NAV Kontroll har ikke et eget saksbehandlingssystem eller fagstøttesystem for sine kontrollsaker. Datatilsynet vil bemerke at det trolig vil være vanskelig for NAV Kontroll å tilfredsstille kravene til behandling av personopplysninger i lov og forskrift uten å etablere en fagapplikasjon som vil erstatte bruk av Access, elektroniske filmapper og papirmapper. Datatilsynet vil sterkt anbefale at dette gjøres.

Tilsynet fant at det ikke er iverksatt tilfredsstillende tiltak for å sikre *konfidensialiteten* på opplysningene. Det vises til at det ikke var iverksatt tiltak for å hindre eller avdekke uautorisert utlevering av personopplysninger fra filmappesystemet. Det er heller ikke iverksatt tiltak for å hindre uautorisert innsyn i personopplysninger som er registrert i filmappesystemet og i Accsess. Dette anses å være brudd på personopplysningslovens § 13 jf forskriftens §§ 2-14 og 2-11.

De samme systemene mangler også tiltak for å beskytte *integriteten* til registrerte opplysninger. Det er påkrevd å treffe tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig, jf. personopplysningsforskriften § 2-13, 1. ledd.

Vedtak om pålegg

Med hjemmel i personopplysningslovens § 46 fatter Datatilsynet følgende vedtak:

1. NAV plikter å etablere planlagte og systematiske tiltak i henhold til personopplysningslovens § 14, for å sikre at kun behandler personopplysninger i forbindelse med sin kontrollvirksomhet i tråd med vilkårene i folketrygdlovens § 21-4, 21-4a og 21-4c, jf. kontrollrapportens punkt 5.1.4 og 5.1.6. Fristen settes til 1. desember 2012. De nye rutinene skal oversendes Datatilsynet.
2. NAV plikter å etablere rutiner i henhold til personopplysningslovens § 14 for å informere **de registrerte** i samsvar med personopplysningslovens § 19 og 20, om den behandling av personopplysninger som skjer med hjemmel i folketrygdlovens kontrollbestemmelser. Rutinene må sikre at unntaksbestemmelsene vurderes konkret og løpende for den enkelte behandling, jf. kontrollrapportens punkt 5.2.5. Fristen settes til 1. desember 2012. De nye rutinene skal oversendes Datatilsynet.
3. NAV må etablere rutiner i henhold til personopplysningslovens § 14 jf dennes § 19 for å sikre at den kontrollerte gis korrekt og fullstendig informasjon om hvordan et **opplysningspålegg** med hjemmel i § 21-3 kan oppfylles. Det må også gis informasjon om hvilke rettigheter vedkommende har som registrert, herunder om retten til å be om innsyn i allerede innsamlede opplysninger jf personopplysningslovens § 18, jf. kontrollrapportens punkt 5.2.5. Fristen settes til 1. desember 2012. De nye rutinene skal oversendes Datatilsynet.
4. NAV skal gi informasjon i samsvar med personopplysningslovens § 20 første ledd jf § 19, til **personer som er eller har vært gjenstand for kontroll** hos NAV, etter personopplysningslovens ikrafttredelse, og hvor det har skjedd en innhenting av personopplysninger om vedkommende. Dette gjelder allikevel ikke i de tilfeller hvor det kan dokumenteres at vedkommende allerede er informert gjennom direkte kontakt med NAV eller Politiet. NAV må foreta en konkret vurdering av om unntakene i § 23 er oppfylt, i de sakene som ikke er avsluttet når vedtaket skal gjennomføres, jf. kontrollrapportens punkt 5.2.5. Fristen settes til 1. mars 2013. En rapport fra dette arbeidet skal oversendes Datatilsynet innen 15. mars 2013.
5. Informasjonssikkerhet
    a. Virksomheten må **dokumentere tilfredsstillende informasjonssikkerhet** ved at det utarbeides risikovurdering i samsvar med personopplysningsloven § 13, jf. personopplysningsforskriften §§ 2-4, jf. kontrollrapportens punkt 5.6.2.1.
    b. Virksomheten må innføre **tilfredsstillende tilgangsstyring** for egen database og elektroniske filmapper. Tilgangsstyringen skal være personlig og knyttes til tjenestelig behov for tilgang til personopplysninger, jf. personopplysningsforskriften §§ 2-7 og 2-8, 3. ledd, jf. kontrollrapporten punkt 5.5.2.2
    c. NAV Kontroll må sette i verk tiltak for å **sikre konfidensialitet** og **forhindre ureglementert innsyn i personopplysninger**, jf. personopplysningsforskriften § 2-11, 1. ledd, jf. kontrollrapportens punkt 5.5.3

d. NAV Kontroll må sette i verk tiltak for å **forhindre og oppdage forsøk på uautorisert utlevering**, jf personopplysningsforskriften § 2-14, 1. og 2. ledd, jf. kontrollrapportens punkt 5.5.3

e. NAV Kontroll må sette i verk tiltak for å **forhindre oversendelse av sensitive personopplysninger over åpne kanaler** som e-post, jf. personopplysningsforskriften § 2-11, 3. ledd. Slike tiltak vil for eksempel være å etablere klare myndighets- og ansvarsforhold med kommunikasjonspartnere, jf. personopplysningsforskriften § 2-15, 4. ledd og å benytte sikker elektronisk kommunikasjon, jf. personopplysningsforskriften § 2-15, 1. ledd, jf. kontrollrapportens punkt 5.6.3.3

6. Internkontroll og sletting

   a. NAV Kontroll må **etablere rutiner for internkontroll**. Dette skal blant annet inneholde rutiner for innsyn, retting, sletting og sikkerhetsrevisjon, jf. personopplysningsloven § 14 og personopplysningsforskriften §§ 2-5, jf. kontrollrapportens punkt 5.7.3.

   b. NAV Kontroll må **etablere en arkivjournal** for tipsarkivet på papir. Dette er nødvendig for å kunne gjennomføre den registrertes rettig til innsyn i egne opplysninger, jf. personopplysningsloven § 18, jf. kontrollrapportens punkt 5.3.3 og 5.3.2.1

   c. Det må etableres en rutine for **systematisk sletting** av elektroniske mapper, jf. personopplysningsloven § 11, litra e, jf. kontrollrapportens punkt 5.3.3 og 5.3.2.3.

Klageadgang
Dette vedtaket kan påklages i henhold til forvaltningslovens bestemmelser. Eventuell klage må fremsettes overfor Datatilsynet **innen tre uker** etter at vedtaket ble mottatt. Datatilsynet gjør i den forbindelse oppmerksom på at direktoratet har rett til innsyn i sakens dokumenter, jf. forvaltningsloven § 18.

Personvernnemnda er klageorgan, og skal behandle saken dersom Datatilsynet ikke finner grunn til å gjøre om sitt eget vedtak.

Med vennlig hilsen

Helge Veum
avdelingsdirektør

Cecilie Rønnevik
fagdirektør

Vedlegg: endelig kontrollrapport