Datatilsynet

Endelig kontrollrapport		
Saksnummer: 12/00116 Dato for kontroll: 07.03.2012 Rapportdato: 22.08.2012	Kontrollobjekt: NAV Direktoratet Sted: NAV Kontroll, og NAV Kontroll Øst	Utarbeidet av: Cecilie L B Rønnevik Marius Engh Pellerud Helge Veum

1 Innledning

Datatilsynet gjennomførte kontroll hos NAV Direktoratet 7. mars 2012. Kontrollen ble utført med hjemmel i personopplysningslovens § 44, jf. § 42, 3. ledd.

Temaet for kontrollen var behandling av personopplysninger som NAV gjennomfører i forbindelse med sin kontrollvirksomhet. Kontrollen fant sted ved NAV Kontroll sentralt, og NAV Kontroll Øst.

I det følgende vil Datatilsynet beskrive de faktiske forhold som ble avdekket under kontrollen. Kontrollrapporten danner grunnlag for Datatilsynets vurderinger og eventuelle pålegg.

2 Tilstede under kontrollen

2.1 Fra virksomheten

- Magne Fladby, direktør for NAV Kontroll
- Bjørg N. Saksæther, seniorrådgiver styringsenheten
- May Snedsbøl, avdelingsdirektør NAV Kontroll Øst
- Haakon Hertzberg, fungerende seksjonssjef juridisk seksjon, Arbeids- og velferdsdirektoratet

2.2 Fra Datatilsynet

- Helge Veum, avdelingsdirektør Tilsyns- og sikkerhetsavdelingen
- Marius Engh Pellerud, rådgiver Tilsyns- og sikkerhetsavdelingen
- Cecilie Rønnevik, seniorrådgiver, Juridisk avdeling

3 Generelt

NAV Kontroll er en spesialenhet i Arbeids- og velferdsetaten. Enhetens hovedoppgave er å føre kontroll med at de utbetalinger som finner sted i henhold til folketrygdlovens bestemmelser er korrekte og rettmessige, og å avdekke eventuelt misbruk av velferdsordningene. Enheten har også ansvaret for å anmelde misbrukssaker til politiet

Datatilsynet legger til grunn at *forvaltningsloven* i utgangspunktet vil komme til anvendelse for hele eller deler av NAVs kontrollvirksomhet. Loven er ment å ivareta borgernes *rettssikkerhet* i forbindelse med forvaltningsutøvelse, og gir rettigheter blant annet til parter i forvaltningssaker. Disse rettighetene er til en viss grad sammenfallende med rettigheter som den registrerte har i henhold til personopplysningsloven, herunder krav om formell

kompetanse hos forvaltningen, og krav om informasjon og kontradiksjon. Forvaltningsloven sikrer også at det føres *kontroll* med forvaltningens praksis, blant annet gjennom klagesaksbehandling og domstolsprøvning – den alminnelige forvaltningskontroll.

Selv om det ligger klart utenfor Datatilsynets mandat å ta stilling til om forvaltningsloven etterleves i forbindelse med NAVs kontrollsaker, tillater Datatilsynet seg å stille spørsmål ved om loven etterleves i forbindelse med innhenting av opplysninger i saker om kontroll av enslige forsørgere[1]. Med bakgrunn i tilsynets observasjoner på dette punktet, blir en kopi av foreliggende rapport og varsel om vedtak oversendt til Sivilombudsmannen for eventuell oppfølgning.

4 Nærmere om gangen i en kontrollsak

4.1 Hvordan en kontroll initieres

NAV Kontroll er mottaker av alle *tips* om misbruk av trygdeytelser, både de som kommer fra eksterne og fra NAV-systemet selv. NAV Kontroll Øst mottar alene ca 2000 tips i året. Det enkelte tips vurderes med hensyn til troverdighet og alvorlighet. Dette skjer blant annet gjennom oppslag i NAVs egne registre. Det gjøres ikke ytterligere kontrollhandlinger dersom tipset er åpenbart grunnløst, for eksempel hvor den som det tipses om ikke mottar den aktuelle stønaden.

Andre saker initieres med i opplysninger fra *forvaltningssakesbehandlingen* i NAV-systemet forøvrig og fra *registerkoblinger*[2].

Hvorvidt, og hvordan, et tilfelle følges opp i NAV Kontroll varierer ut fra stønadstype og omstendighetene for øvrig:

- Enkelte saker overføres direkte til forvaltningssaksbehandling, med tanke på å treffe vedtak om opphør og eventuelt tilbakebetaling av ytelse. Dette gjelder hvor faktum er tilstrekkelig avklart og det ikke ellers er grunn til å se nærmere på saken. Saken kan samtidig anmeldes til politiet.
- I andre saker vil det være behov for ytterligere undersøkelser, før det tas stilling til om det er grunnlag for forvaltningssaksbehandling og eventuell straffereaksjon. I den forbindelse gjøres det ytterligere kontrollhandlinger ved kontrollenheten.

Datatilsynet har sett nærmere den videre gangen i to kontrollkategorier: kontroll med enslige forsørgere og kontroll med behandlende helsepersonell, jf pkt 4.2 og 4.3.

4.2 Nærmere om kontroll av enslige forsørgere

Enslige forsørgere har rett til en rekke ytelser i henhold til folketrygdloven, for eksempel tilskudd til barnepass. NAV gjennomfører kontrollhandlinger med sikte på å *avdekke om*

---

[1] Enhetens rutiner for kontroll av enslige forsørgere reflekterer ikke forvaltningslovens bestemmelser om forberedelse ved enkeltvedtak (§§ 16 flg), eller om opplysningspålegg og granskning (jf lovens §§ 14 og 15). Den standardteksten som et utarbeidet for innkalling til personlig samtale med stønadsmottager inneholder ikke informasjon om klageadgang etter § 14.

[2] Registerkoblinger omhandles særskilt, jf rapportens pkt 5.4

stønadsmottaker faktisk lever sammen med barnets andre forelder, og henter inn opplysninger for å belyse dette.

Disse vil for en stor del være personopplysninger om *stønadsmottaker* og *den andre forelderen*. I visse tilfeller hentes det inn opplysninger om *andre* enn stønadsmottaker og den andre forelderen, for eksempel gjøres det oppslag i folkeregisteret på andre beboere i det som er angitt å være den andre forelderens bolig.

Opplysningene hentes fra

- *NAVs* egne saksbehandlingssystemer
- *Internett*, offentlig tilgjengelig informasjon som for eksempel Facebook
- andre *offentlige organer*, for eksempel skatteetaten og de registrertes bostedskommune
- offentlige og private *virksomheter*, typisk fra bank, post- og ekomleverandører
- *andre personer* i stønadsmottakers omkrets, typisk ansatte i barnets barnehage, borettslaget, utleier av bolig, og i visse tilfeller fra stønadsmottakers og den andre forelderens naboer, venner og familie
- *stønadsmottaker* og den andre *forelderen*[3]

Under kontrollen fremkom det at opplysningene ble hentet inn både gjennom skriftlige henvendelser, og muntlig - typisk gjennom telefonsamtaler. I henhold til rutinene skal det lages et skriftlig referat fra gjennomførte telefonsamtaler, som skal inngå i saksmappen. Dersom det ikke fremkommer relevante opplysninger blir det, i henhold til hva saksbehandlere opplyste, normalt ikke laget et telefonreferat[4].

I enkelte tilfeller blir stønadsmottaker kalt inn til en personlig samtale for å opplyse saken. Dette omhandles særskilt under pkt 5.1.1.5.

4.3 Nærmere om kontroll av behandlende helsepersonell

Behandlende helsepersonell avgir erklæringer som legges til grunn i stønadssaker hvor det foreligger medisinske vilkår for rett til ytelse. I tillegg har helsepersonellet en viktig rolle i forbindelse med refusjons- og tilskuddsordninger, for eksempel i de tilfeller hvor helsehjelp skal betales delvis av pasienten selv og delvis av NAV. Det er i slike tilfeller helsepersonellet som søker refusjon fra NAV.

For det første gjennomfører NAV kontrollhandlinger med sikte på *å avdekke hvorvidt de medisinske erklæringene som ligger til grunn for en stønad er korrekte*. Dette vil typisk gjelde sykepenger. Slike kontroller retter seg gjerne mot både pasienten og helsepersonellet.

---

[3] Opplysningspålegg behandles særskilt, jf rapportens pkt 5.1.5 og 5.1.6

[4] I sitt tilsvar til varsel om vedtak forklarer NAV at det lages et telefonreferat fra alle samtaler, også i de tilfelle hvor saken ikke tilføres relevante opplysninger

Det hentes inn opplysninger for blant annet å belyse pasientenes reelle helsetilstand og oppholdssted, og legens oppholdssted, hans økonomi[5] og generelle praktisering. Det hentes derved inn personopplysninger, både om *helsepersonellet* og dennes *pasienter*.

Opplysningene hentes fra

- *NAVs* egne saksbehandlingssystemer
- *annet helsepersonell*, for eksempel i form av pasientjournaler (hele eller deler)
- *andre pasienter*
- andre *offentlige organer*, for eksempel skatteetaten, HELFO og Tollvesenet
- offentlige og private *virksomheter,* typisk bank
- fra pasientens *arbeidsgiver*
- fra *stønadsmottaker og helsepersonellet* selv[6]

Under kontrollen opplyste saksbehandlerne at opplysningene ble hentet inn både gjennom skriftlige henvendelser, og muntlig - typisk gjennom telefonsamtaler. I henhold til rutinene skal det lages et skriftlig referat fra telefonsamtaler, som skal inngå i saksmappen. Dersom det ikke fremkommer relevante opplysninger blir det etter det normalt ikke laget et telefonreferat[7].

I enkelte tilfeller blir stønadsmottaker kalt inn til en personlig samtale for å opplyse saken. Dette omhandles særskilt under pkt 5.1.1.5.

4.4 Kort om den videre kontrollgjennomføringen

Saksbehandlerne ved NAV Kontroll skal løpende vurdere hvorvidt det skal hentes inn flere opplysninger i saken, eller om den anses ferdig opplyst.

Når saken er ferdig opplyst kan den få ulike utfall:

- Saken overføres til forvaltningssaksbehandling, enten ved NAV kontroll eller ved forvaltningen for øvrig. Resultatet kan bli stans og/eller tilbakebetaling av ytelsene.
- Saken anmeldes til politiet
- Saken underlegges forvaltningssaksbehandling *og* anmeldes – samtidig eller sekvensielt
- Saken "henlegges", det vil si at den avsluttes uten ytterligere utreding/reaksjon

4.5 Informasjonsbehandling og bruk av informasjonssystem

NAV Kontroll anvender i dag flere ulike systemer i sin saksbehandling. NAV kontroll mangler et enhetlig fagsystem for området. Dette oppleves som en svakhet av enheten selv. Enheten benytter NAVs generelle saksbehandlingsverktøy Gosys, et tipsarkiv i Microsoft

---

[5] I sitt tilsvar konkretiserer NAV at det hentes inn opplysninger fra legens bank kun i de tilfeller hvor det er mistanke om at legen oppholder seg i utlandet og det i samme tidsrom er skrevet en legeerklæring i hans navn. En slik praksis er ikke dokumentert i virksomhetens rutiner.

[6] Opplysningspålegg behandles særskilt, jf rapportens pkt 5.1.5 og 5.1.6.

[7] I sitt tilsvar til varsel om vedtak skriver NAV at det ikke hentes inn opplysninger muntlig fra behandler. Dersom behandler selv tar kontakt i saken skrives imidlertid et notat fra samtalen.

Access utviklet i egen organisasjon, et papirarkiv og elektroniske mapper på de ansattes filområder. Systemstøtten på området framstår som fragmentert. Konsekvenser av dette er potensial for dobbeltlagring, manglende gjenfinning og sporbarhet, samt manglende helhetlige sikkerhetsvurderinger.

En overordnet grafisk framstilling av rutiner og systemer i NAV Kontroll framkommer i vedlegg 1 til denne rapporten. Funksjoner, rutiner og systemer som anses som del av NAV Kontroll er innenfor avrundet firkant. Systemer som benyttes i NAV Kontrolls saksbehandling som også benyttes av andre deler av NAV er definert innenfor NAV Kontroll. Andre enheter i NAV er definert som utenfor NAV Kontroll.

4.6 Sentrale fagsystemer i NAV

NAV har en rekke fagsystemer som benyttes i sin saksbehandling. De mest sentrale beskrives kort under[8].

Gosys er en felles arbeidsflate for saksbehandlere på tvers av fagsystemene for å fange opp aktiviteter, oppgavebehandling, fordeling av oppgaver, skanning og journalføring av dokumenter med mer.

Infotrygd er saksbehandlingssystemet som gir støtte i vedtak og utbetalingsprosess for de fleste av saksområdene til tidligere Trygdeetaten. Systemet har grensesnitt mot de fleste av NAVs systemer.

PESYS er etatens verktøy for veiledning og saksbehandling på pensjonsområdet.

BISYS er saksbehandlingssystemet for bidragssaker.

Arena er et oppfølgingsverktøy som benyttes i NAV, blant annet i forbindelse med saksbehandling av arbeidsavklaringspenger. Arena benyttes til å behandle søknader, utbetaling og oppfølging av den enkelte klient.

4.7 Tipsarkivet - Access

NAV Kontroll har utviklet et system for registrering av *tips* om trygdemisbruk. Systemet er utviklet i Microsoft Access og omtales i etaten som Access. Her registreres i tillegg til tipset også *videre aktiviteter* i saken, som oversendelse av rapport om saken, vedtak om henleggelse, samt registrering av vedtak fra andre forvaltningsorgan og fra politi og domstol. Access har vært brukt i NAV Kontroll til registrering av tips siden 2008. Fram til det ble tips registrert i NAV-fylkeslinja i Excel og Infotrygd.

Det er kun saksbehandlere med rollen "koordinator" som har tilgang til å registrere opplysninger i Access. Databasen er sikret ved at kun koordinatorene har tilgang til filmappen der databasen er lagret[9]. I tillegg er basen passordbeskyttet ved pålogging. Det benyttes ett felles passord til basen for hver region. Ingen saksbehandlere har landsdekkende tilgang til

[8] Systemene er nærmere beskrevet i kontrollsak 11/00797
[9] NAV: "Lagring av tips og anmeldelser i Access"

databasen, men alle med tilgang til basen kan sjekke om enkeltpersoner er registrert av andre enheter.

4.8 Arkiv og journal

NAV Kontroll har papirbasert nærarkiv og fjernarkiv. Aktive saker oppbevares i nærarkivet, avsluttede saker overføres til fjernarkivet. Saksmappene er arkivert på fødselsnummeret til personen som mistenkes for trygdemisbruk. PID-nummeret som tilordnes i Access påføres sakene i papirarkivet. Mappene der er organisert etter årstall, og påført den kontrollertes fødselsnummer.

Det fins ingen journal for arkivet, verken på papir eller elektronisk. Under kontrollen ble Datatilsynet gjort kjent med at Riksarkivet har ført kontroll med etatens arkivdanning, og at det er gitt en rekke pålegg om utbedringer.

4.9 Elektroniske mapper

Løpende saksbehandling og logging av aktiviteter i en sak føres av den enkelte saksbehanlder i excel. Excel-loggen og andre dokumenter i saken lagres i elektroniske mapper. Mappenes navn er fødselsnummeret på personen som kontrolleres i hver enkelt sak.

4.10 Manuell behandling av personopplysninger

I samtale med saksbehandlerne ved enheten fikk tilsynet opplyst at det i stor utstrekning hentes inn opplysninger fra tredjepersoner via telefon.

Datatilsynet mener at det er svært viktig med etterprøvbarhet i kontrollsakene, slik at det er mulig å finne tilbake til hvilke kontrollhandlinger som er gjennomført og hva disse resulterte i, av positive og negative funn. I den utstrekning det hentes inn opplysninger via telefonsamtaler er det derfor nødvendig at det sikres en grad av notoritet fra samtalene, for eksempel ved at det føres et referat som inngår som dokument i saken. Dette muliggjør en etterkontroll av forvaltningens virksomhet, og er nødvendig for at den kontrollerte skal kunne kreve partsinnsyn og innsyn etter personopplysningsloven. Datatilsynet legger til grunn at alle samtaler blir registrert i Accsess, som nevnt under pkt 4.7.

Tilsynet ønsker å presisere personopplysningsloven gjelder fullt ut for opplysninger som skal inngå i saken, eller registreres på en slik måte at opplysningene blir gjenfinnbare, jf personopplysningslovens § 3. Dette gjelder selv om innhentingen i seg selv er manuell, for eksempel skjer i en telefonsamtale.

5 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

5.1 Det rettslige grunnlaget for kontrollhandlinger som innebærer behandling av personopplysninger

5.1.1 Legalitetsprinsippet

En behandling av personopplysninger er i prinsippet et tiltak som innebærer et inngrep i den enkeltes privatliv. Det følger av EMK artikkel 8, av EUs personverndirektiv og av

personopplysningslovens § 11 at en behandling av personopplysninger derfor krever rettslig grunnlag. I henhold til legalitetsprinsippet skal det rettslige grunnlagets styrke og klarhet stå i forhold til hvor inngripende den aktuelle behandlingen er.

Spørsmålet om rettslig grunnlag faller i to deler: For det første må det avklares hvilket rettslig grunnlag som kreves for den aktuelle behandlingen, jf opplistingen i personopplysningslovens §§ 8 og 9. Dernest må det vurderes hvorvidt et slikt grunnlag faktisk foreligger. I begge disse henseende vil legalitetsprinsippet være et førende tolkningsprinsipp.

5.1.2 Hvilket rettslig grunnlag kreves?

Datatilsynet legger til grunn at NAV sin behandling av personopplysninger i kontrolløyemed må ha *hjemmel i lov.*

I den forbindelse har tilsynet lagt vekt på at *formålet* med tiltakene er å føre kontroll med enkeltpersoners etterlevelse av et regelverk hvor lovbrudd er belagt med straff, at behandlingen skjer som ledd i offentlig *forvaltningsutøvelse*, og er *påtvunget* den enkelte. Når behandlingen medfører *spredning* av personopplysninger vil kravet til det rettslige grunnlaget skjerpes. Det samme gjelder i de tilfeller hvor behandlingen også omfatter *sensitive* personopplysninger.

Lovhjemmel sikrer normalt at *forholdsmessigheten*[10] i de ulike tiltakene belyses og avveies gjennom en demokratisk lovprosess. Lovhjemmel gir i tillegg *forutberegnlighet* for borgerne, med hensyn til hvilke opplysninger om vedkommende som blir behandlet, når, av hvem og for hvilke formål. Dette er informasjon som er nødvendig blant annet for at den enkelte skal kunne ivareta sine rettigheter i forbindelse med behandlingen.

5.1.3 Generelt om de relevante kontrollhjemlene – innhenting av opplysninger fra andre enn medlemmet

I denne forbindelse er det særlig kontrollbestemmelsene i folketrygdlovens § 21-4 og § 21-4a og § 21-4c som er relevante[11].

Folketrygdlovens § 21-4 gir etaten hjemmel til å hente inn opplysninger "som er *nødvendige* for å kontrollere om vilkårene for en ytelse er eller har vært oppfylt i tilbakelagte perioder". Opplysningene kan etter denne bestemmelsen bare hentes inn fra en nærmere oppregnet krets av personer og virksomheter. Dersom det foreligger *rimelig grunn til mistanke* om at det har skjedd eller vil skje urettmessige utbetalinger fra trygden utvides etatens kompetanse. I medhold av § 21-4a kan det da hentes inn nødvendige opplysninger fra enhver, og også opplysninger som gjelder andre enn stønadsmottaker.

I § 21-4c gis det enkelte bestemmelser vedrørende etatens innhenting av opplysninger. Her gis det nærmere vilkår for innhenting av pasientjournal. I tillegg oppstilles enkelte formkrav til innhentingen, herunder oppstilles en plikt til å informere om formålet med innhentingen og å vise til relevante hjemler.

---

[10] Jf proporsjonaliteskravet i EMK art 8

[11] Bestemmelsen om medlemmets opplysningsplikt i lovens § 21-3 vil bli behandlet nedenfor.

Stortinget har på dette området gitt forvaltningen svært vide fullmakter[12]. Store deler av forholdmessighetsvurderingene er overlatt til forvaltningens eget skjønn. Slik lovgivningsteknikk kan ha gode grunner for seg. Lovgiver vil ikke alltid ha realkompetanse til å kunne vurdere hvilke opplysninger som er nødvendige. I tillegg kan detaljert lovregulering skape en uhensiktsmessig statisk rettstilstand.

Stortinget forutsetter imidlertid eksplisitt at forvaltningen faktisk gjør de forholdmessighetsvurderinger[13] som er foreskrevet, og vurderer konkret hvorvidt innhentingen er nødvendig[14] og hvorvidt det foreligger mistanke[15]. Behandlinger som er uforholdsmessige, eller som finner sted uten en forutgående forholdsmessighetsvurdering, vil ikke ha hjemmel i nevnte bestemmelser.

Det er pr i dag ikke utarbeidet *forskrifter* til disse bestemmelsene i folketrygdloven. Departementet har således ikke foretatt egne forholdsmessighetsvurderinger, som munner ut i mer konkrete retningslinjer for opplysningsbehandlingen.

Nærmere bestemmelser om kontrollgjennomføringen er gitt i Arbeids- og velferdsetatens eget *rundskriv*[16] *til § 21-4*. Rundskrivet gir i liten grad uttrykk for overordnede forholdsmessighetsvurderinger: Nødvendighetsvurderingen overlates for en stor del til den enkelte saksbehandlers eget skjønn, jf avsnittet "Nødvendige opplysninger", uten at det samtidig er gitt nærmere føringer for skjønnsutøvelsen. På ett punkt kan rundskrivet endog leses slik at nødvendighetsvilkåret erstattes med et vilkår om hensiktsmessighet[17]. Selv om mistankekravet i § 21-4a er omhandlet i rundskrivet er det etter tilsynets vurdering lite veiledning å hente for hvordan mistanken skal vurderes i det konkrete tilfellet.

Det er også utarbeidet et *rundskriv til § 21-4c*, hvor det blant annet gis særlige bestemmelser for innhenting av pasientjournal. Tilsynet har ingen kommentarer til disse. Rundskrivet inneholder også generelle regler for innhenting av opplysninger. Disse er å anse som formkrav, og ikke direkte relevante i denne forbindelse.

I tillegg et det et *rundskriv* kalt Retningslinjer for behandling av saker om trygdemisbruk. Rundskrivet gir i hovedsak føringer for enhetens videre behandling av en sak etter at det er avdekket eller konstatert misbruk, og gir ikke føringer som er direkte relevante i denne forbindelse.

Det følger av dette at de *interne rutinene* i NAV Kontroll får avgjørende betydning, når det gjelder å sørge for at de tiltakene som iverksettes i det enkelte tilfellet er lovlige. Det må derved stilles strenge krav til rutinene.

---

[12] Det forhold at lovhjemlenes ordlyd er så vidtrekkende som i dette tilfellet har også betydning for spørsmålet om informasjonsplikt til de registrerte. Dette omhandles nærmere i rapportens pkt 5.2.

[13] for å oppfylle vilkårene i EMK art 8
[14] Ftl § 21-4 og § 21-4a
[15] Ftl § 21-4a
[16] R-21-00-2-111
[17] Jf punktet "Spesielt om opplysninger fra forsikringsselskap"

De interne rutinene i NAV Kontroll gjengir folketrygdlovens vilkår om nødvendighet og mistanke, men gir liten veiledning i hvordan disse vilkårene skal vurderes. Normalt må det kunne forventes at de personvernulempene som skal tas i betraktning i det enkelte tilfellet identifiseres.

Når det gjelder enslige forsørgere lister rutinene opp en rekke steder hvor det kan hentes opplysninger. Samtidig opplyses det at listen bare angir eksempler, og at "det gjøres oppmerksom på at listen ikke er uttømmende".

Det er etablert egne rutiner for innhenting av pasientjournal og for innhenting av opplysninger fra finansinstitusjoner. Disse inneholder klarere grenser for opplysningsbehandlingen enn de generelle rutinene. Det bemerkes også at rutinene for kontroll av mulig svart arbeid gjennomgående gir bedre veiledning enn rutinene for kontroll med enslige forsørgere.

5.1.4 Konklusjon om kontrollhjemler

Datatilsynet vil bemerke at de tiltak som NAV iverksetter for å kontrollere den enkelte i mange tilfeller er svært inngripende. Det er imidlertid vanskelig å vurdere hvorvidt den behandlingen som NAV gjennomfører i kontrolløyemed har hjemmel i nevnte bestemmelser. Det vises til at det er vanskelig for tilsynet å belyse og etterprøve hvilke vurderinger som er gjort i det enkelte tilfellet, med hensyn både til *nødvendighet* og *mistanke* om misbruk.

Datatilsynet mener det er uheldig at forholdsmessighetsvurderingen som foreskrives i EMK art 8 i så stor utstrekning overlates til den enkelte saksbehandlers eget skjønn. Det kan ikke ses bort fra at saksbehandleren selv vil ha problemer å identifisere og ta i betraktning de forhold som taler imot at behandlingen iverksettes. Med mindre kontrollen overføres til forvaltningsbehandling vil enhetens vurderinger heller ikke være gjenstand for alminnelig forvaltningskontroll i henhold til forvaltningslovens bestemmelser, for eksempel klagesaksbehandling.

Datatilsynet etterlyser klare rammer for NAVs saksbehandlere, hva gjelder innhenting av personopplysninger i kontrolløyemed. De interne rutinene ved NAV Kontroll er ikke tilfredsstillende for å sikre at enhetens behandling av personopplysninger skjer i henhold til personopplysningslovens krav om rettslig grunnlag, jf dennes § 11 litra a jf §§ 8 og 9. Dette er et brudd på personopplysningslovens krav om internkontroll, jf denne lovs § 16.

Tilsynet vil sterkt anbefale at NAVs kontrollvirksomhet reguleres nærmere i *lov eller forskrifts* form, slik at rammene for virksomheten blir klarere enn hva som er tilfelle i dag. Etter tilsynets vurdering er dette nødvendig for å sikre at forvaltningen ivaretar grunnleggende menneskerettigheter og internasjonale forpliktelser i hvert enkelt tilfelle.

5.1.5 Særlig om opplysningspålegg

I forbindelse med en kontroll vil NAV kunne ha behov for opplysninger direkte fra den som mottar ytelsen. I den forbindelse er det tradisjonelt benyttet såkalte *"egenerklæringer"*, et slags spørreskjema som fylles ut av stønadsmottaker. Det finnes også rutiner for å be om

opplysninger i brevs form, slik at man utber en nærmere *skriftlig forklaring* fra stønadsmottaker om de forhold man ønsker belyst.

Under kontrollen ble det opplyst at disse undersøkelsesmetodene er stadig mindre brukt overfor *stønadsmottaker*, typisk overfor enslig forsørger. Det ble opplyst at man i større grad innkaller stønadsmottaker til *samtaler*. Slike samtaler foregår ved personlig fremmøte enten på det lokale NAV-kontoret eller i NAV Kontroll sine lokaler. Manglende fremmøte til en slik samtale vil kunne medføre at den aktuelle ytelsen stanses, jf folketrygdlovens § 21-7.

Skriftlig innhenting blir brukt gjennomgående når det er *helsepersonell* som kontrolleres. Eventuelle samtaler gjennomføres i henhold til det opplyste pr telefon, og det føres referat fra samtalen.

I henhold til folketrygdlovens § 21-3 annet ledd kan NAV kreve at den som mottar eller har mottatt en ytelse *gir de opplysninger eller legger frem de dokumenter* som en nødvendige for å kontrollere ytelsens størrelse eller vilkårene for rett til ytelse. Datatilsynet kan vanskelig se at denne bestemmelsen gir NAV adgang til å pålegge den som kontrolleres å *møte til en samtale* med de ansatte i NAV. Bestemmelsen sier kun at opplysningene skal gis, men gir ingen anvisning på hvordan opplysningene avgis.

Det må legges til grunn at det å stille i en samtale med saksbehandlere fra NAV oppleves som et mer inngripende tiltak enn det er å avgi en skriftlig erklæring. Det må tas i betraktning at det foreligger en mistanke om at loven brytes, og at samtalen har til formål å avdekke hvorvidt vedkommende bryter loven.

En slik samtale vil etter omstendighetene fort kunne bære preg av å være et slags avhør. Det vises i den forbindelse til enhetens eget dokument "Forslag til samtaledisposisjon". Dokumentet gir anvisning på klassisk avhørsmetodikk. Det gis blant annet anvisning på hvordan man skal holde tilbake opplysninger fra den som forklarer seg, for å konfrontere vedkommende med opplysningene på et senere tidspunkt. Formålet er å avdekke uriktige forklaringer fra stønadsmottaker.

5.1.6 Konklusjon om opplysningspålegg

Det er tvilsomt hvorvidt tilsynet har kompetanse til å fatte vedtak vedrørende NAVs praktisering av bestemmelsen om opplysningspålegg. Datatilsynet tillater seg allikevel å stille spørsmål ved denne.

Slik tilsynet forstår bestemmelsen har den kontrollerte adgang til å gi opplysninger og dokumentasjon både muntlig og skriftlig. Det er etter tilsynets vurdering ikke grunnlag for å pålegge den kontrollerte å stille til samtale gjennom personlig oppmøte.

Tilsynet viser forøvrig til rapportens pkt 5.2.4 om etatens informasjonsplikt etter personopplysningsloven.

5.2 Informasjonsplikt ved innhenting av personopplysninger i kontrolløyemed

5.2.1 Generelt om informasjonsplikten

Den registrertes rett til informasjon om behandling av personopplysninger er grunnleggende. Informasjon er en nødvendig forutsetning for at den registrerte skal kunne ivareta sine rettigheter, herunder å kreve innsyn, retting og sletting.

Personopplysningslovens §§ 19 og 20 om informasjonsplikt gjelder i utgangspunktet for de behandlinger som NAV iverksetter i kontrolløyemed, jf også presiseringen i folketrygdlovens § 21-4c fjerde ledd. Datatilsynet legger videre til grunn at personopplysningslovens unntaksbestemmelser i § 20 annet ledd og § 23 for opplysninger er relevante når NAV henter inn personopplysninger med hjemmel i nevnte bestemmelser[18].

Når det hentes inn personopplysninger plikter den behandlingsansvarlige som hovedregel å gi den registrerte *informasjon som er nødvendig for at han skal kunne ivareta egne rettigheter* etter loven, jf § 19. I det minste skal den registrerte ha informasjon om navn og adresse på behandlingsansvarlig, hva som er formålet med behandlingen, om opplysningene vil bli utlevert og eventuelt hvem som er mottaker, og hvorvidt det er frivillig å gi fra seg opplysningene.

Når opplysningene skal hentes *fra den registrerte selv* må informasjonen gis før opplysningene hentes inn, jf § 20. I de tilfeller hvor opplysningene hentes *fra andre* enn den registrerte oppstår informasjonsplikten først når opplysningene er hentet inn, med mindre formålet med innhentingen er å gi dem videre til andre. Da kan informasjonen gis først når utlevering skjer.

5.2.2 Kort om praksisen ved NAV Kontroll

Under kontrollen opplyste NAV at det ikke ble gitt informasjon til den registrerte ved innhenting av andre opplysninger enn pasientjournal[19]. Dette gjenspeiles også i enhetens rutiner for kontroll av enslige forsørgere og for kontroll ved mistanke om svart arbeid.

Dette medfører i praksis at den registrerte først får kunnskap om at det har vært hentet inn opplysninger om ham når han enten

- mottar et *varsel om vedtak i en forvaltningssak,* typisk om stans og/eller tilbakebetaling av stønad,
- *pålegges å gi opplysninger* i medhold av folketrygdlovens § 21-3, eller
- mottar *henvendelse fra politiet,* med bakgrunn i en anmeldelse som er levert

[18] Jf tolkningsuttalelse fra Justis- og beredskapsdepartementet av 31. mai 2011 (201013088 EP KMV)

[19] NAV har etablert særlige rutiner for å gi informasjon ved innhenting av *pasientjournal*. Datatilsynet har ingen merknader til disse.

I de mange tilfeller hvor kontrollen ikke resulterer i en forvaltningssak eller i en anmeldelse, og hvor det heller ikke hentes inn opplysninger fra den registrerte selv, vil den registrerte *aldri* få informasjon om den behandlingen som har funnet sted.

5.2.3 Nærmere om informasjonsplikt ved innhenting fra andre enn den registrerte

NAV henter inn betydelige mengder personopplysninger fra andre enn den registrerte, med hjemmel i folketrygdlovens § 21-4 og § 21-4a. Dette gjelder både for kontroll som retter seg mot den registrerte selv, og når kontrollen retter seg mot andre (typisk helsepersonell).

Under kontrollen viste NAV til unntaket i **personopplysningslovens § 20 annet ledd litra a,** hvoretter informasjonsplikten etter § 20 ikke gjelder for behandling som er *"uttrykkelig fastsatt i lov"*[20].

For at en lovhjemmel skal kunne sette til side informasjonsplikten etter personopplysningslovens § 20 jf § 19, må ordlyden i den aktuelle hjemmelen være så klar at den setter den enkelte i stand til med en viss grad av sikkerhet å forstå hvorvidt det faktisk behandles opplysninger om vedkommende, hvilke opplysninger som eventuelt behandles, når dette skjer og til hvilket formål osv.

Datatilsynet er av den av den oppfatning at ordlyden i både folketrygdlovens § 21-4 og § 21-4a er svært vid[21]. Det foreligger heller ingen forskriftsregulering, som gir nærmere informasjon om behandlingen.

Bestemmelsene gir etter sin ordlyd *minst to behandlingsansvarlige* fullmakt til *når som helst,* og *fra en svært stor krets av personer og aktører,* å hente inn *enhver personopplysning* som NAV finner nødvendig for sin kontroll. Så vide hjemler er vurdert å være nødvendig for at staten skal ha tilfredsstillende kontroll med utbetaling av trygdeytelser. Konsekvensen er imidlertid at lovhjemlene får begrenset informasjonsverdi; de angir et handlingsrom som blir så stort at det ikke er mulig å forutsi med en viss grad av sikkerhet hvilke kontrollhandlinger som rent faktisk gjennomføres i henhold til hjemmelen.

Datatilsynet kan vanskelig se at en registrert gjennom å lese bestemmelsen blir i stand til å overskue *hvorvidt* det faktisk hentes inn opplysninger om ham til kontrollformål, og i så fall *når* skjer, *hvilke* opplysninger som hentes inn og *hvor* opplysningene hentes fra.

Datatilsynets mener at de konkrete hjemlene i dette tilfellet er for vide til at de kan sies å "uttrykkelig fastsette" enhver opplysningsinnhenting som NAV gjør for kontrollformål, på en slik måte at informasjonsplikten faller bort *i ethvert tilfelle.* Hvorvidt unntaket kommer til anvendelse må derved bero på en *konkret forholdsmessighetsvurdering* i det enkelte tilfellet: jo mer inngripende behandlingen er, desto klarere må lovhjemmelen være.

Opplysningenes art og omfang må være sentrale elementer i forholdsmessighetsvurderingen.

---

[20] Datatilsynet har tidligere vurdert hvorvidt folketrygdlovens § 21-4 uttrykkelig hjemler innhenting av pasientjournaler, på en slik måte at informasjonsplikten faller bort etter personopplysningslovens § 20 annet ledd litra a. Datatilsynets saksnummer 09/01032.

[21] Jf også tilsynets vurderinger i denne rapportens pkt 5.1.1

I de tilfeller hvor kontrollen retter seg mot den registrerte, må det i tillegg tas hensyn til at *formålet med innhentingen* er å føre kontroll med dennes etterlevelse av et regleverk som er belagt med straff. Hensynet til kontradiksjon må i slike tilfeller veie tungt.

Det må også tas hensyn til hvorvidt innhentingen (indirekte) medfører en *spredning* av opplysninger, og det må tas særlig hensyn til eventuell spredning i den registrertes omkrets. Det at NAV Kontroll henvender seg til personer i den kontrollertes omkrets og ber om opplysninger vil medføre en spredning av sensitive opplysninger om vedkommende. Nemlig om at han er mistenkt for en straffbar handling, jf personopplysningslovens § 2 nr 8. Det forhold at opplysninger om at man er mistenkt for trygdemisbruk tilflyter ens borettslag og barnehage er noe man bør informeres om.

Under kontrollen viste NAV også til faren for bevisforspillelse, og anførte at informasjonsplikten uansett måtte anses bortfalt i henhold til **personopplysningslovens § 23 første ledd litra b**. Bestemmelsen unntar fra informasjonsplikten i de tilfeller hvor det er "påkrevd med hemmelighold av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger".

Datatilsynet er av den oppfatning at heller ikke denne hjemmelen gir grunnlag for å unnta fra informasjonsplikten *i ethvert tilfelle* hvor NAV henter inn personopplysninger for kontrollformål. Hvorvidt lovens vilkår er oppfylt må også her bero på en konkret forholdsmessighetsvurdering. Jo mer inngripende behandlingen er, desto sterkere står informasjonsplikten[22].

Tilsynet vil i den forbindlese peke på at uttrykket "påkrevd" er et skjerpet nødvendighetsvilkår, som tilsier at unntaket skal anvendes med *stor forsiktighet*.

For at bestemmelsen kommer til anvendelse må det i utgangspunktet foreligge *konkrete holdepunkter* i det enkelte tilfelle, som tyder på at det å gi informasjon vil medføre at formålet med behandlingen blir vanskelig- eller umuliggjort. Det vil ikke være tilfelle når den registrerte ikke har reell mulighet til å påvirke innhentingen, typisk hvor opplysningene skal hentes fra den registrertes bank eller hans pasientjournal.

Endelig vil tilsynet peke på at bestemmelsen i praksis kun gir anvisning på en *utsatt* informasjonsplikt. Når faren for bevisforspillelse er bortfalt, skal informasjonen gis. Bestemmelsen kan således ikke gjøre unntak fra informasjonsplikten i de tilfeller hvor saken er avsluttet ved en "henleggelse" hos NAV Kontroll.

5.2.4 Nærmere om informasjonsplikt ved innhenting fra den registrerte selv

NAV henter inn personopplysninger fra den registrerte selv, både skriftlig og muntlig. Datatilsynet har sett nærmere på den informasjonen som gis i forbindelse med innkalling til samtale vedrørende ytelser som enslig forsørger. Den oppfyller langt på vei de minimumskrav som følger av personopplysningslovens § 19.

---

[22] Jf over

Det gis imidlertid ikke informasjon om hvilke opplysninger som etaten eventuelt *har innhentet* om vedkommende på et tidligere stadium i saken, for eksempel fra tredjepersoner jf over. Tvert imot gir rutinene[23] anvisning på at saksbehandler aktivt bør holde tilbake informasjon om hvilke opplysninger man sitter med, for å bruke disse i en konfrontasjon under samtalen.

Etter tilsynets vurdering gis det heller ikke tilfredsstillende informasjon om hvorvidt det er frivillig eller ikke å avgi opplysninger *gjennom en samtale*, jf § 19 første ledd litra d. Basert på den informasjon som gis om medlemmets medvirkningsplikt i innkallingen, kan det lett trekkes en slutning om at det er obligatorisk å møte til en samtale. Den som ikke møter vil i tillegg få et varsel om at den aktuelle ytelsen stanses med mindre vedkommende stiller i henhold til ny innkalling. Som nevnt over mener Datatilsynet at folketrygdlovens § 21-3 ikke gir hjemmel for å pålegge medlemmet å oppgi opplysninger i en samtale.

5.2.5 Konklusjon vedrørende informasjonsplikt

NAV sin praksis med å unnlate informasjon til de registrerte er i strid med kravene i personopplysningslovens §§ 19 og 20 jf unntakene i personopplysningslovens § 20 annet ledd litra a og § 23 første ledd litra b.

NAV må endre sine rutiner for å sikre at det foretas en *konkret vurdering* i hvert enkelt tilfelle av hvorvidt lovens unntaksbestemmelser kommer til anvendelse. Dette gjelder både for fremtidige kontrollsaker, og for saker som er løpende og avsluttede ved NAV Kontroll.

Loven gir uansett ikke adgang for NAV til å holde tilbake opplysninger i den hensikt å senere kunne konfrontere den kontrollerte med dem i en personlig samtale. Informasjonsplikten etter personopplysningslovens § 19 innebærer tvert imot en plikt for NAV til å gi den registrerte all informasjon som er nødvendig for at han skal kunne ivareta sine rettigheter etter loven på best mulig måte, for eksempel be om innsyn i allerede innsamlede opplysninger.

Dersom det gis et opplysningspålegg overfor den registrerte selv, med hjemmel i § 21-3, må det gis korrekt og fullstendig informasjon om hvordan opplysningspålegget kan oppfylles. Den informasjonen som gis i dag må endres, for å tilfredsstille informasjonsplikten i personopplysningsloven.

5.3 Sletting av personopplysninger

5.3.1 Generelt om sletteplikten

I henhold til personopplysningslovens § 28 skal ikke den behandlingsansvarlige oppbevare personopplysninger lengre enn et som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning skal de slettes.

NAV er utvilsomt underlagt arkivlovens bestemmelser, og plikter å oppbevare alt arkivverdig materiale.

---

[23] Jf etatens eget "Forslag til samtaledisposisjon"

5.3.2 Praktisering av regelverket

5.3.2.1 Funn - Access

Tidligere slettet NAV alle åpenbart grunnløse tips. Denne praksisen ble avsluttet etter at Riksarkivet påla etaten å avslutte praksisen med å slette slike tips[24]. Dette pålegget må imidlertid ses i lys av Riksarkivets andre krav i samme dokument. Riksarkivet stiller i samme dokument krav om at NAV utarbeider arkivplan, og bevarings- og kassasjonsplan. En lagring av ubegrunnede tips uten at innholdet i Arkivverkets samlede krav er oppfylt synes urimelig. Konsekvensene vil da, som i dag, være lagring av til dels svært sensitive personopplysninger uten at disse er enkelt tilgjengelige, for eksempel i forbindelse med at den registrerte ber om innsyn i henhold til personopplysningslovens bestemmelser.

Rutiner for anonymisering av regulert i eget dokument[25]. Dokumentet er utformet av NAV kontroll og regulerer anonymiseringen av tips som skjer i Access. Grunnløse tips skal anonymiseres umiddelbart. Saker som henlegges i avklaringsfasen skal anonymiseres etter 6 måneder (for å unngå dobbeltregistrering og for å kunne fange opp flere tips på samme person i perioden). Saker som oversendes andre myndigheter anonymiseres 6 måneder etter oversendelse. Ettersom anonymisering skjer i juli og februar vil lagringstiden overstige 6 måneder. Dokumentet framstår i tråd med rutiner slik de ble beskrevet på stedlig kontroll.

Anonymiseringen foregår ifølge etaten ved at etternavn og fødselsnummer slettes. Det opprinnelige tipset arkiveres på papir og påføres et identifiseringsnummer fra registreringen i Access (PID). Papirtipset oppbevares personidentifisert og kan knyttes til den anonymiserte saken i Access ved hjelp av PIDen. Datatilsynet vil bemerke at dette ikke er å anse som en reell anonymisering, og at tipsene kan identifiseres ved bruk av PID.

Papirtipsene oppbevares i en perm på kontoret til en person i NAV Kontroll. Papirtipsene er organisert kronologisk ut fra tidspunktet for registrering. Dette forhindrer i praksis gjennomføring av innsyn for den registrerte, da det ikke fins noen identifisert journal for sakene.

Anonymiseringen skjer på ulike tidspunkt avhengig av oppfølgingen av tipset. Når tips viser seg å være grunnløse, som regel fordi det viser seg at NAV ikke utbetaler den aktuelle ytelsen til personen tipset omhandler, skal tipset anonymiseres umiddelbart.

Saker som henlegges i avklaringsfasen skal anonymiseres etter seks måneder. Dette for å forhindre dobbeltregistrering og for å kunne fange opp flere tips på samme person innenfor en kort periode. Saker som oversendes andre myndigheter skal anonymiseres etter seks måneder fra oversendelse. Det framgår av stedlig kontroll at anonymisering for henlagte saker skjer i halvårlige kjøringer. Det innebærer at i praksis vil enkelte saker være identifisert i Access opptil nesten et år etter henleggelse.

---

[24] Riksarkivets saksnr 2011/686 Endelig tilsynsrapport og pålegg om utbedringer

[25] NAV: "Anonymisering i Access"

5.3.2.2 Funn - Arkiv og journal

Når en sak er endelig skal det ryddes i saken før saken arkiveres[26]. Her fastslås det at dokumenter som er hentet fra interne fagsystemer skal makuleres. Det samme gjelder overskuddsinformasjon (informasjon som ikke er etterspurt og/eller ikke har verdi som dokumentasjon i saken). Overskuddsinformasjon kan eventuelt sladdes om det anses som mer hensiktsmessig.

5.3.2.3 Funn - Elektroniske mapper

Enheten for strafferettslig vurdering har en rutine for sletting av elektroniske mapper ved henleggelse[27]. Ut over dette framstår det som det ikke gjennomfører systematisk sletting av slike mapper.

5.3.3 Konklusjon vedrørende sletting og arkivering

Riksarkivet[28] har konkludert med at NAV blant annet må utarbeide en bevarings- og kassasjonsplan for alt arkivverdig materiale.

Manglende etterlevelse av arkivlovgivningens bestemmelser om oppbevaring og kassasjon medfører i dette tilfellet også brudd på personopplysningslovens § 28 om sletting. Det vises til at det i utgangspunktet foreligger en sletteplikt for opplysninger som ikke inngår i virksomhetens arkiv.

For denne rapportens vedkommende legger tilsynet 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.

Datatilsynet vil for øvrig vise til kontrollrapportens kap 5.2.3 og 5.2.5 vedrørende *informasjonsplikt*. Tilsynet vurderer det slik at systematisk innhenting og oppbevaring av tips er en behandling som utløser informasjonsplikt i henhold til personopplysningslovens § 20.

5.4 Registerkontroll

For å avdekke trygdemisbruk og feilutbetalinger gjennomfører NAV Kontroll koblinger mellom egne og andre etaters registre. Følgende kontroller har vært gjennomført og gjennomføres av NAV Kontroll:

- Inntektskontroll av pensjonister
  Informasjon om inntekt hentes fra Skatteetaten. Data kobles med NAVs registre om pensjonsutbetalinger.
- Kontroll av mottakere av dagpenger og arbeidsavklaringspenger
  Mottakere av stønad knyttes mot AA-registeret for å avdekke eventuelle arbeidsforhold mens vedkommende mottar trygdeytelser.
- Inntektskontroll av enslige forsørgere

[26] NAV: Rutine for journalføring/ registrering, arkivering og kassasjon av fagpost i NAV Kontroll, kontrollenhetene

[27] NAV: Arbeidsbeskrivelse ved strafferettslige vurderinger – per 05.03.12

[28] Riksarkivets saksnummer 2011/686

Inntektsdata fra skatteetaten kobles mot mottakere av stønad til enslige forsørgere. Avdekker overskridelse av inntektsgrensen.

- Kontroll av inntektsgrunnlaget til mottakere av sykepenger
  Innrapportert inntektsgrunnlag fra sykemeldt person kobles med faktisk inntekt fra skatteetaten.
- Kontroll av utvidet barnetrygd
  Mottaker av utvidet barnetrygd kobles mot folkeregisteret for å avdekke annen sivilstatus enn innmeldt.

Ved registerkontroll bestiller NAV Kontroll filuttrekk fra eget direktorat ved behov. Lønns- og trekkoppgaver hentes årlig fra Skatteetaten. Filuttrekk behandles i en MS Access-database og kobles ved hjelp av fødselsnummer.

Kildefiler og resultat etter kobling lagres fram til sakene er ferdigbehandlet. Internkontroll og sikkerhetsrutiner for disse filene behandles i avsnitt 5.7.2.

Datatilsynet har i brev til Arbeidsdepartementet datert 9. desember 2011 tatt opp flere forhold rundt NAVs kontrollhjemler. Problemstillinger rundt registerkontroll var ikke videre tema for kontrollen.

5.4.1 Håndtering av personopplysninger i forbindelse med listekontroller

NAV Kontroll har utformet en rutinebeskrivelse for oppbevaring og sletting av data i forbindelse med listekontroller[29]. Formålet med dokumentet er å sørge for at listekontrolldata slettes når det ikke er behov for dem. Dokumentet beskriver hvilke kontrolldata som er sensitive og hvordan og hvilke data som skal hentes inn. Det stilles krav om at data skal hentes via et lukket fil-område og skal overføres til "UtviklerPC". Det er ikke beskrevet andre krav til datasikkerhet. Det er beskrevet at data skal oppbares ut året etter at data ble innhentet. Dette innebærer at data kan oppbevares opp til nesten to år etter innhenting.

5.5 Informasjonssikkerhet – Registrering og arkivering

5.5.1 Krav i regelverket

Personopplysningslovens § 13 stiller krav om den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet.

Personopplysningsforskriftens kapittel 2 gir utfyllende bestemmelser. Her nevnes blant annet:

- § 2-3 om sikkerhetsledelse, med konkrete krav om etablerte sikkerhetsmål og strategi,
- § 2-7 om organisering, og klare ansvars- og myndighetsforhold,
- § 2-8 om personell og fastlagte rutiner,
- § 2-6 om avviksbehandling, og
- § 2-5 om sikkerhetsrevisjoner.

For sikkerhetsforhold gjelder også internkontrollplikten etter lovens § 14.

---

[29] NAV: Rutine for innhenting, oppbevaring og sletting av sensitive data i forbindelse med listekontroller

5.5.2 Funn

5.5.2.1 Funn - Arkiv og journal

Det fins ingen journal for arkivet, verken på papir eller elektronisk. Datatilsynet vil anføre at dette er i strid med krav om journalføring i arkivforskriften § 2-6, men oppfølging av dette regelverket er utenfor Datatilsynets mandat.

5.5.2.2 Funn - Elektroniske mapper

Mappene er tilgjengelig for flere saksbehandlere med oppgaver på samme fagområde, men ikke tilgjengelig for andre i enheten. Det er ingen egen pålogging for tilgang til mappene. Det er ingen sperrer i systemet som forhindrer at filer med sensitiv informasjon kan distribueres ut av etaten ved bruk av for eksempel mail eller lagringsmedier over USB (minnepinne eller ekstern harddisk) for ansatte med nødvendige rettigheter.

5.5.3 Vurdering

Personopplysningene NAV Kontroll behandler er alle relatert til potensielle lovbrudd. Dette er tilfelle også der mottak av trygdeytelser og –refusjoner skjer på bakgrunn av feil, ikke bare faktiske forsøk på svindel. I tillegg vil NAV gjennomgående behandle opplysninger om noens helseforhold. Personopplysningene NAV Kontroll behandler vil derfor være å anse som sensitive jf. personopplysningsloven § 2, litra b.

Opplysninger om at personer er registrert av NAV Kontroll er i seg selv krenkende ettersom det antyder at personen har vært involvert i mulig lovbrudd. Ut over dette innehar NAV Kontroll store mengder personopplysninger om de personene NAV foretar undersøkelser av, blant annet familieforhold, bruk av teletjenester og bankforhold og økonomi. I sum gir mengden personopplysninger NAV Kontroll besitter et omfattende bilde av personlige forhold som vil kunne oppfattes som krenkende. Konsekvensene ved sikkerhetsbrudd vil derfor måtte sies å være store. Sikkerhetsnivået for beskyttelse av slike data må kunne kreves å være tilsvarende høyt, jf. personopplysningsforskriften § 2-1, 2. ledd.

Den behandlingsansvarlige har plikt til å sikre personopplysninger på en måte som står i forhold til sannsynligheter og konsekvenser av sikkerhetsbrudd, jf. personopplysningsforskriften § 2-1, 2. ledd. Konsekvenser er spesielt høye om sikkerhetsbrudd kan føre til tap av liv og helse, økonomisk tap eller tap av anselse og personlig integritet, jf. personopplysningsforskriften § 2-1, 1. ledd. Virksomheten skal også fastlegge kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. personopplysningsforskriften § 2-4, 1. ledd. Datatilsynet har ikke mottatt noen slik vurdering.

Når konfidensialitet er påkrevd skal det treffes tiltak for å forhindre innsyn i personopplysninger, jf. personopplysningsforskriften § 2-11, 1. ledd. Datatilsynet vurderer dagens løsning til at konfidensialiteten til registrerte personopplysninger ikke i tilstrekkelig grad er ivaretatt. NAV Kontroll tilfredsstiller heller ikke regelverkets krav om sikkerhetstiltak som hindrer eller sikrer oppdagelse av forsøk på uautorisert utlevering, jf personopplysningsforskriften § 2-14, 1. og 2. ledd.

Det er påkrevd å treffe tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig, jf. personopplysningsforskriften § 2-13, 1. ledd. Datatilsynet anser det som NAV Kontroll mangler tiltak for å beskytte integriteten til registrerte personopplysninger.

Datatilsynet vurderer det slik at det må etableres tiltak som hindrer uautorisert uthenting av eller endring av personopplysninger. For eksempel kontroll over nettverksdeling eller annen særskilt kontroll med beskyttelsesverdigeopplysninger.

5.5.4 Konklusjon

Bruk av elektroniske mapper og Access avviker fra regelverkets krav om konfidensialitet, jf. personopplysningsforskriften § 2-11, 1.ledd, avviker fra regelverkets krav om integritetsbeskyttelse, jf. personopplysningsforskriften § 2-13, 1. ledd, mangler nødvendige sikkerhetstiltak, jf. personopplysningsloven § 2-11, 1. og 2. ledd og sikkerhetsnivået er ikke vurdert i forhold til sannsynlighet og konsekvens av sikkerhetsbrudd, jf. personopplysningsloven § 2-1, 2. ledd.

5.6 Risikovurderinger

5.6.1 Krav i regelverket

Personopplysningslovens § 13 stiller krav om at virksomheten etablerer tilfredsstillende informasjonssikkerhet gjennom planlagte og systematiske tiltak.

Personopplysningsforskriftens stiller krav om at virksomheten dokumenterer tilfredsstillende informasjonssikkerhet gjennom bruk av risikovurderinger, jf. § 2-4. Den behandlingsansvarlige plikter selv å sette kriterier for akseptabel risiko, og vurdere sine løsninger opp mot disse.

Det stilles videre krav om at ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

5.6.2 Funn

Datatilsynet har etterspurt risikovurderinger fra NAV Kontroll. Dokumentasjon av gjennomførte risikovurderinger er ikke oversendt. Det er derfor grunn til å tro at risikovurderinger dermed ikke er gjennomført for bruken av elektroniske mapper og Access.

5.6.2.1 Konklusjon

Manglende risikovurderinger er et avvik fra kravene i personopplysningsforskriftens § 2-4, 2. ledd.

5.6.3 Informasjonssikkerhet ved kommunikasjon med andre parter

5.6.3.1 Krav i regelverket

For kommunikasjon over media utenfor den behandlingsansvarliges kontroll, stiller forskriftens § 2-11 krav om at slik kommunikasjon skal krypteres eller sikres på annen måte. I praksis medfører dette at kommunikasjon av identifiserbare beskyttelseverdige personopplysninger må krypteres dersom de kommuniseres over for eksempel e-post eller telefaks.

5.6.3.2 Funn

NAV offentliggjør e-post-adressene til kontrollenehetene på sine hjemmesider. Selv om det på hjemmesidene står eksplisitt at sensitive personopplysninger ikke skal sendes per mail, ble det avdekket under kontrollen at NAV Kontroll mottar sensitive opplysninger på e-post. Det at publikum sender inn sensitive opplysninger på e-post er det vanskelig å sikre seg mot. Under kontrollen ble det imidlertid oppdaget flere arkiverte e-poster fra politiet med senstiv informasjon.

5.6.3.3 Konklusjon

Når konfidensialitet er nødvendig skal personopplysninger krypteres ved elektronisk forsendelse, jf. personopplysningsforskriften § 2-11, 3. ledd. Bruk av usikret e-post er ukryptert og må anses som helt åpent for utenforstående. Den behandlingsansvarlige har ansvar for å etablere klare ansvars- og myndighetsforhold med kommunikasjonspartnere ved elektronisk kommunikasjon, jf. personopplysningsforskriften § 2-15, 4. ledd.

Det er den behandlingsansvarlige som er subjektet for disse reglene. Samtidig må mottakere av forsendelser, ved gjentatte brudd på regelverket, forventes å reagere. NAV Kontroll bør etablere klare avtaleforhold med aktører som jevnlig avgir sensitive opplysninger. Slike avtaler åpner også for elektronisk utveksling av sensitive opplysninger, jf. personopplysningsforskriften § 2-15, 1. ledd.

Datatilsynet anser jevnlig mottak av sensitive opplysninger fra andre offentlige aktører over usikrede kanaler, som politiet, som et avvik fra personopplysningsforskriften § 2-11, jf 2-15

5.7 Internkontroll

5.7.1 Krav i regelverket

Personopplysningslovens § 14 oppstiller krav om at den behandlingsansvarlige skal etablere planlagte og systematiske tiltak for å sikre at personopplysningslovens bestemmelser etterleves ved behandlingen (internkontroll). Utfyllede bestemmelser er gitt i personopplysningsforskriftens § 3-1.

5.7.2 Funn

Datatilsynet er i forbindelse med kontrollen oversendt tre dokumenter som kan sies å regulere internkontroll i NAV Kontroll. Dette er "Sikkerhetsgjennomgang i NAV. Operativ retningslinje", "Rutine for journalføring/ registrering, arkivering og kassasjon av fagpost i NAV Kontroll, kontrollenhetene" og "Anonymisering i Access".

Dokumentene kan etter tilsynets vurdering ikke sies å være dekkende for rutinebehovet etter personopplysningslovens § 14. Blant annet mangler dokumentasjon av følgende:

- Rutiner for innsyn, retting og sletting
  Kun rutiner for anonymisering i Access er dokumenter. Det ble under stedlig kontroll vist til "rydding i sak". Det ble også vist til sletting av elektroniske mapper av enheter for strafferettslig vurdering. Dette vurderes som utilstrekkelig.
- Kontrollerende rutiner

NAV Direktorat stiller krav om at lokale enheter skal etablere kontrollerende rutiner. Datatilsynet kan ikke se at dette er gjort i NAV Kontroll.

5.7.3 Konklusjon

Datatilsynet anser at NAV Kontroll ikke har etablert planlagte og systemtiske tiltak for i sikre at personopplysningslovens bestemmelser etterleves ved behandlingen (internkontroll). Forholdet anses som et brudd på personopplysningslovens § 14, jf. personopplysningsforskriftens 3. kapittel.

Vedlegg

- Grafisk skisse over rutiner og systemer i NAV Kontroll