Tilgangskontroller i NAV

Gjennomgang, analyse og forslag til forbedringer

Oslo, 31. oktober 2016

BDO

Wiersholm

Innhold

DEL I INNLEDNING 3

1. INNLEDNING OG OPPSUMMERING 3

2. OM GJENNOMGANGEN 6
   2.1 Tildeling av oppdraget og mandat 6
   2.2 Forståelse og løsning av mandatet 6
   2.3 Personvern 7
   2.4 Beskrivelse av arbeidsmetode 7

DEL 2 OM NAV 10

3. ORGANISERING 10

4. SAKSBEHANDLINGSKRAV 11
   4.1 Krav til behandling av personopplysninger 11
   4.2 Krav til informasjonssikkerhet og internkontroll 12
   4.3 Øvrige krav til NAVs saksbehandling 13

5. SIKKERHETSARBEIDET I NAV 14
   5.1 Innledning 14
   5.2 Sikkerhetsseksjonen 15
   5.3 Sikkerhetskoordinator og sikkerhetsmedarbeider 15
   5.4 Internrevisjonen 15

6. TILGANG TIL OG BRUK AV FAGSYSTEMER 16
   6.1 NAVs Fagsystemer 16
   6.2 Vilkår for tilgang til Fagsystemer 17
   6.3 Nærmere om tilgangskontroll 19

DEL 3 PRAKTISK ETTERLEVELSE AV PERSONVERNLOVGIVNINGEN 21

7. OPPSLAG UTEN TJENSTLIG BEHOV 21
   7.1 Innledning 21
   7.2 Oppslag på offentlig kjente personer 21
   7.3 Oppslag på seg selv, relasjoner og kollegaer 22
   7.4 Oppslag på bekjente 22
   7.5 Oppslag ved ansettelser i NAV 23

8. BRUK AV LOGGER 23

9. REAKSJONSMØNSTER 23
   9.1 Innledning 23
   9.2 Manglende oversikt over saker 24
   9.3 Manglende enhetlig reaksjonsregime 25

10. STYRINGSSYSTEMET 25
   10.1 Innledning 25
   10.2 Overordnede Sikkerhetskrav 26
   10.3 Felles Sikkerhetsnormer 27
   10.4 Styringsdokumentet 28

10.5 Operative retningslinjer 29
10.6 Vurdering av styringssystemet 30
10.7 Særlig om innebygd personvern 31
10.8 Håndtering av avvik 32
10.9 Opplæring og kjennskap til regelverket 33

DEL 4 ANBEFALINGER 35

11. OVERORDNET 35

12. ENDRING I ORGANISERINGEN AV PERSONVERNARBEIDET 35

13. FORBEDRING AV STYRINGSSYSTEMET 36

14. SYSTEMATISKE LOGGANALYSER 38

15. IMPLEMENTERING OG OPPLÆRING 38

16. ENHETLIG REAKSJONSMØNSTER 39

DEL I INNLEDNING

1. INNLEDNING OG OPPSUMMERING

Arbeids- og velferdsetaten er en statlig etat under Arbeids- og velferdsdirektoratet som igjen sorterer under Arbeids- og sosialdepartementet. Sammen med sosialtjenestene i kommunene inngår etaten i arbeids- og velferdsforvaltningen ("**NAV**"). NAV står i en særstilling i Norge; både i kraft av forvaltning av én tredjedel av det norske statsbudsjettet, som en av landets største arbeidsgivere, og som en forutsetning for velferdsmodellen vårt samfunn bygger på. Så å si alle borgere i Norge er i kontakt med NAV i løpet av sine liv. Med et så betydelig samfunnsoppdrag følger en rekke forpliktelser.

NAVs hovedforpliktelser er gjennomføring av arbeidsmarkeds-, trygde- og pensjonspolitikken i Norge. Dette innebærer å få mennesker i arbeid, holde dem i arbeid, samt å forvalte og utbetale om lag 60 ulike stønader og ytelser. I 2015 leverte NAV tjenester til ca. 2,8 millioner mennesker og utbetalte samlet sett ca. 450 milliarder kroner. NAVs driftsbudsjett i 2015 var på ca. 11,6 milliarder kroner.

Med de oppgaver NAV er pålagt følger behandling av personopplysninger i et enormt omfang. I forvaltningen og ved bruk av flere saksbehandlingssystemer behandler NAV svært mange sensitive personopplysninger, eksempelvis opplysninger om helseforhold og opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling. I tillegg behandler NAV en svært stor mengde personopplysninger hvor konfidensialitet og forsvarlig saksbehandling er tilsvarende nødvendig, eksempelvis informasjon om familieforhold, familierelasjoner og informasjon om en persons økonomiske forhold samt informasjon om personer med adressesperre begrunnet i fare for "skade på liv, legeme eller helse".

For NAVs ansatte innebærer dette blant annet at den enkelte medarbeider ikke skal behandle personopplysninger som er uvedkommende for den enkeltes utførelse av sine pålagte arbeidsoppgaver. I NAV er dette gjennomgående definert og regulert gjennom bruk av normen "tjenstlig behov".

De norske reglene om personvern er forankret i Den europeiske menneskerettighetskonvensjonen og Grunnloven. De konkrete prinsipper og regler er nedfelt i personopplysningsloven som suppleres av en rekke forskrifter[1]. Alle virksomheter i Norge har et selvstendig ansvar for å etterleve relevante personvernsrettslige regler og prinsipper. Dette er i økende grad en forpliktelse som tillegges den enkelte aktør. Forpliktelsene vil forsterkes ytterligere ved den nært forestående implementeringen av EUs nye personvernforordning i norsk rett.

I februar 2016 ble NAV kjent med at en ansatt hadde misbrukt sin tilgang til personopplysninger i NAVs saksbehandlingssystemer. Situasjonen foranlediget en personalsak hvor ansettelsesforholdet ble avsluttet. NAV har også tidligere opplevd liknende saker av ulik karakter og omfang. På denne bakgrunn tok arbeids- og velferdsdirektøren initiativ til en gjennomgang med det formål å kartlegge omfang av uberettigede oppslag; samt å vurdere statlige styringssystemer, tilgangskontroller, rutiner og retningslinjer for personvern og informasjonssikkerhet; samt praktisk etterlevelse av disse i NAV. Revisjonsselskapet BDO AS ("**BDO**") og Advokatfirmaet Wiersholm AS ("**Wiersholm**") innga felles tilbud 2. mars 2016, og ble tildelt oppdraget 1. april 2016.

Et viktig bakteppe for gjennomgangen har vært at NAV over flere år gjennom rapporter fra både Riksrevisjonen, Datatilsynet og NAVs internrevisjon har fått informasjon som

[1] Personopplysningsloven er den norske implementeringen av EUs personverndirektiv (Direktiv 95/46/EF) av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

klart tilsier at deres behandling av personopplysninger ikke er tilfredsstillende. I tillegg har media gjennom en rekke artikler over flere år omtalt NAVs behandling av personopplysninger. Flere konkrete tiltak og handlingsplaner har blitt utarbeidet som følge av dette.

Strategisk fokus: Det er BDOs og Wiersholms overordnede vurdering og konklusjon at NAV ikke har evnet, i tilstrekkelig grad, å forstå betydningen av at behandling av personopplysninger står sentralt i NAVs virksomhet og hvilke strenge krav som følger av dette. NAV har flere ganger blitt gjort oppmerksom på forhold som burde foranlediget at brukernes personvern og behandling av personopplysninger ble løftet på den strategiske agenda og dermed gitt arbeidet med å ivareta brukernes personvern den nødvendige prioritet. Dette synes ikke å være gjort.

Gjennomgangen viser at personvern, herunder tilgangskontroll og problemstillinger om uberettigede oppslag, jevnlig har vært på agendaen i NAV og at NAV de siste årene har styrket sitt arbeid med personvern. Det er BDOs og Wiersholms oppfatning at mange medarbeidere har god forståelse av regelverket og at den relevante lovgivning og de interne regelverk etterleves av det store flertall av medarbeidere i NAV.

Undersøkelsen viser like fullt at uberettigede oppslag utgjør en utfordring i NAV.[2] Undersøkelsene har avdekket behov for korrigerende tiltak på tvers av organisasjonen. Utfordringene som er avdekket har flere og sammensatte forklaringer.

BDOs og Wiersholms viktigste observasjoner som blant annet følger av manglende strategisk fokus på personvern og behandling av personopplysninger i NAV, er oppsummert gjennom nedenstående fem punkter. Alle foreslåtte tiltak har en økonomisk side. De vil på linje med alle andre tiltak i NAV være gjenstand for prioriteringer. Det er imidlertid BDOs og Wiersholms klare oppfatning at en rekke av de forhold som påpekes vil kunne avhjelpes/utbedres ved hjelp av forholdsmessige og moderate ressurser sett i forhold til viktighet.

Organisatoriske utfordringer: Systemundersøkelsen har avdekket organisatoriske utfordringer i relasjon til arbeid med personvern og informasjonssikkerhet.

Utfordringen kan i stor utstrekning begrunnes i en sammenblanding av kontrollerende og utøvende funksjoner. Sikkerhetsseksjonen er i dag organisert som en rapporterende enhet under IKT-seksjonen. Medarbeidere rapporterer direkte til IKT-direktøren. I praksis betyr dette at Sikkerhetsseksjonen, som er ansvarlig for at styringssystemet følges, organisatorisk er plassert under en direktør som skal følge det samme styringssystemet.

Sikkerhetsseksjonens nåværende ressurser og organisering anses ikke robust nok til å ha det ansvaret de per i dag har for personvern i NAV. Ressursene bør styrkes. Det anbefales at Sikkerhetsseksjonen omorganiseres til en avdeling som blant annet skal ha det overordnete ansvaret for NAVs arbeid med personvern og informasjonssikkerhet. Denne avdelingen bør plasseres på stabsnivå i organisasjonen, og avdelingsdirektøren bør ha en direkte rapporteringslinje til arbeids- og velferdsdirektøren. I denne avdelingen må det avsettes dedikerte ressurser med ansvar for personvern. Det anbefales videre at Sikkerhetskoordinatfunksjonen styrkes. De lokale sikkerhetskoordinatorers roller må være klart definert i en stillingsbeskrivelse, og det må avsettes tilstrekkelig med ressurser for å ivareta disse oppgavene.

BDO og Wiersholm anbefaler også at NAV etablerer et sentralt personvernombud i form av en heltidsstilling med ansvar for å påse at NAV etterlever personvernregelverkets krav. Det bør videre vurderes om det skal etableres flere personvernombud som rapporterer til det sentrale personvernombudet.

[2] Logganalyser har identifisert ulike typetilfeller av oppslag uten tjenstlig behov. Disse funnene underbygges av svar på en omfattende spørreundersøkelse som er sendt ut til samtlige ansatte i NAV.

Behov for forbedring av eksisterende styringssystem: Gjennomgangen har avdekket behov for en forbedring av det eksisterende styringssystemet for personvern, informasjonssikkerhet og beredskap.

En rekke gode styringsdokumenter, sikkerhetskrav og retningslinjer er etablert. Personvern, informasjonssikkerhet og beredskap er samlet i et felles styringssystem. Styringsdokumentet for personvern, informasjonssikkerhet og beredskap henviser til NAVs overordnede mål, men personvern er ikke fremhevet som tilstrekkelig tydelig i NAVs overordnede mål, jf. også overordnet vurdering om strategisk fokus.

NAV har i liten grad en god prosess for å måle om styringssystemet fungerer etter hensikten, og risikostyringsprosessen er ikke tilstrekkelig koblet til styringssystemet. Hensikten med å måle om styringssystemet fungerer er å sørge for kontinuerlig forbedring av prosessene, for å etterleve krav i lov og forskrift og øvrige interne sikkerhetskrav. Da styringssystemet ikke blir målt på en god nok måte risikerer NAV at styringssystemet ikke er i stand til å sørge for at relevante lov- og forskriftskrav følges. Det bør etableres målbare vurderingsparameter som er forankret hos ledelsen. I dette ligger også at lokale ledere bør måles på sitt arbeid med styringssystemet.

Gjennomgangen og anbefalinger i denne rapporten har tatt høyde for en rekke utfordringer knyttet til de ulike systemene, særlig eldre systemer, som er i bruk på tvers av NAV. Arbeid for mer helhetlige løsninger pågår løpende, men det er en kjensgjerning at NAV må forholde seg til systemene slik de til enhver tid er. Det er like fullt BDOs og Wiersholms oppfatning at etablering av et mer helhetlig system for tilgangsstyring ligger innenfor det som er mulig også under de tekniske forutsetninger og økonomiske rammer NAV opererer under.

Mangelfull bruk av logger: Gjennomgangen har avdekket at bruken av logger har vært fragmentert og mangelfull.

NAV sitter på informasjon fra logger som relativt enkelt kan benyttes for å gjennomføre relativt "treffsikre" analyser og kontroller som er velegnet til å avdekke brudd i form av misbruk av tilganger og oppslag uten tjenstlig behov. De undersøkelser BDO og Wiersholm har utført ved hjelp av informasjon fra loggene har avdekket omfang og alvorlighet av brudd i gitte perioder. Det bør arbeides mer målrettet og systematisk med denne logginformasjonen.

Fragmentert og begrenset opplæring: Gjennomgangen har avdekket at opplæring innen tematikken har vært fragmentert og begrenset.

Det har tidligere ikke vært noe obligatorisk opplæring om personvern og informasjonssikkerhet for ansatte. Det må i større grad arbeides kontinuerlig og helhetlig med de ansattes forståelse av hva som ligger i ansvaret for informasjonssikkerhet og personvern, og hvordan dette skal ivaretas i det daglige arbeidet. Opplæring og vedlikehold av kompetanse bør være et kontinuerlig og risikobasert arbeid som er tilpasset de ansattes stilling og funksjon. Opplæringen bør følges opp med jevnlige diskusjoner på sentralt- og enhetsnivå.

Fravær av et klart håndhevingsregime ved brudd: Gjennomgangen har avdekket at håndteringen av de personalmessig krevende spørsmål i praksis er preget av et lokalt delegeringsregime, der den enkelte enhetsleder er ansvarlig for håndteringen av brudd. Oppfølgning fra sentralt hold skjer ikke systematisk, og det er heller ingen systematikk i at de lokale ledere involverer de sentrale organer i vanskelige saker. Én konsekvens av dette er også at NAVs sentrale HR-funksjoner blir ute av stand til å ivareta sitt ansvar på arbeidsgiverområdet. Det bør utformes et enkelt, enhetlig reaksjonsregime for oppslag uten tjenstlig behov. På bakgrunn av manglende oversikt over det totale antall saker, anbefales implementering av obligatorisk rapporteringsplikt når den aktuelle type saker avdekkes.

2. OM GJENNOMGANGEN

2.1 Tildeling av oppdraget og mandat

NAV utlyste oppdraget i februar 2016 under rammeavtale med enkelte konsulentselskaper. Det var en forutsetning at oppdraget ble ledet av konsulentselskapets juridiske avdeling eller at selskapet knyttet til seg et advokatfirma. Oppdraget ble oppgitt å kreve tverrfaglig kompetanse innen personvern, granskning, IKT-systemer samt teknologiske løsninger.

Etter å ha inngitt felles tilbud, ble BDO og Wiersholm tildelt oppdraget. Det endelige mandatet er datert 21. april 2016. Mandatet fastsetter at BDO og Wiersholm skal kartlegge innholdet i, og etterlevelse av, arbeids- og velferdsetatens rutiner for informasjonssikkerhet med utgangspunkt i NAVs saksbehandlingssystemer og med fokus på ansattes tilgang til personopplysninger. Funn skal vurderes opp mot relevante rettsregler og internt regelverk.

Mandatet definerer formålet med gjennomgangen som å avklare hvorvidt Arbeids og velferdsetatens systemer og rutiner, samt etterlevelse i NAV fungerer opp mot det relevante rettslige rammeverk. Det fremkommer eksplisitt at hensikten ikke er å kartlegge eller vurdere ansvarsforhold. Det er heller ikke et mål å avdekke enkelttilfeller av misbruk. Endelig inneholder mandatet føringer knyttet til rapportering, saksbehandlingsregler, rettssikkerhet og personvern.

Gjennomgangen er utført av BDO og Wiersholm under ledelse av advokat (H) og professor II (PhD) Jan Fougner. Advokatene Georg A. Engebretsen, Jannicke Eilertsen, Ragnhild J. Nakling og advokatfullmektig Nicolai Skjold har vært særlig sentrale i Wiersholms arbeidsgruppe. Kristian Thaysen har ledet BDOs arbeidsgruppe. Ingvild Fasting, Ingunn Holte og Frank Skapalen har vært særlig sentrale i BDOs arbeidsgruppe. Det er i stor grad trukket på begge firmaers samlede ressurser i arbeidet.

2.2 Forståelse og løsning av mandatet

Etter BDOs og Wiersholms oppfatning, legger ikke mandatet konkrete føringer for hvordan de nødvendige undersøkelser skal gjennomføres. Det er valgt å legge Advokatforeningens retningslinjer for private granskninger til grunn så langt de passer.[3] Det følger av retningslinjene at gjennomgangen skal være uavhengig, at den skal belyse alle sider av saken og at det skal gis tilgang til relevant informasjon. Hensynet til rettssikkerhet, personvern, verifikasjon, forsvarlighet, objektivitet, uavhengighet og grundighet har vært bærende prinsipper for arbeidet. I tråd med Advokatforeningens regelverk er det utarbeidet egne retningslinjer for gjennomgangen datert 21. april 2016. For øvrig er arbeidet gjennomført i henhold til anerkjente metoder for granskingsarbeid og sikkerhetsrevisjoner.

Mandatet legger opp til at gjennomgangen skal ha særlig oppmerksomhet på *"ansattes tilgang til personopplysninger"*. I dette ligger en henvisning til tilgangskontroll i NAV og oppslag på personopplysninger uten tjenstlig behov. Ved kartleggingen av dette er flere områder av personvernlovgivningen sentral. Det er ikke foretatt en fullstendig vurdering av alle personvernrettslige aspekter ved NAVs virksomhet, da dette faller utenfor mandatet.

Mandatet er tolket slik at oppdraget er begrenset til statlige systemer, rutiner og retningslinjer; mens arbeidet knyttet til etterlevelse omfatter alle sider av NAV.

Mandatet fastsatte at arbeidet skulle leveres så raskt som mulig innenfor fristen 1. september 2016. Mandatet inneholdt en opsjon for forlengelse av fristen til

[3] "Retningslinjer for private granskninger" vedtatt av Advokatforeningens hovedstyre 4. mars 2011.

31. desember 2016. NAV besluttet å forlenge fristen til 31. oktober 2016. Rapporten er datert 31. oktober 2016.

BDO og Wiersholm legger til grunn at herværende rapport besvarer mandatet.

2.3 Personvern

BDO og Wiersholm har vurdert ulike spørsmål knyttet til ivaretakelse av personvern både ved oppstarten av arbeidet og løpende gjennom Systemundersøkelsen. Vilkårene for behandling av personopplysninger er oppfylt, jf. personopplysningsloven § 11 jf. § 8. Det foreligger også grunnlag for behandling av sensitive personopplysninger, jf. personopplysningsloven § 9. Formålet med undersøkelsen har imidlertid ikke vært å undersøke sensitive personopplysninger.

Behandlingen av personopplysninger er meldt Datatilsynet i henhold til personopplysningsloven § 31. Videre er det inngått en databehandleravtale mellom BDO og NAV, samt mellom BDO og Wiersholm.

I tillegg til personvernlovgivningen har BDOs og Wiersholms interne personvernsregelverk og retningslinjer for informasjonssikkerhet blitt overholdt ved behandlingen av personopplysningene.

2.4 Beskrivelse av arbeidsmetode

2.4.1 Samarbeid med NAV

Gjennomgangen ble iverksatt på initiativ fra arbeids- og velferdsdirektør Sigrun Vågeng. Det har vært avholdt flere møter mellom Vågeng, BDO og Wiersholm. Seksjonssjef Haakon Hertzberg har ledet arbeidet på daglig basis. Det har vært et tett og kontinuerlig samarbeid mellom Hertzberg, BDO og Wiersholm gjennom hele prosessen.

BDO og Wiersholm avholdt innledende samtaler med representanter fra NAV før arbeidet ble iverksatt. Formålet med samtalene var å få overordnet informasjon om NAVs saksbehandlingssystemer og den enkelte ansattes tilgang til personopplysninger.

I samarbeid med NAV ble det besluttet å nedsette en ressursgruppe. Ressursgruppen har bestått av syv representanter fra ulike avdelinger og seksjoner i NAV. Formålet med ressursgruppen var å koordinere arbeidet fra NAV sin side samt å sikre informasjonsflyt begge veier. Det er blitt avholdt fremdriftsmøter på løpende basis, i tillegg til annen løpende kontakt. Flere av ressursgruppens medlemmer er også blitt intervjuet av BDO og Wiersholm.

Ressursgruppens medlemmer har fått rapportutkastet tilsendt for gjennomlesning for å sikre at de faktiske forhold i rapporten er korrekt beskrevet. Bemerkninger er gjennomgått og tatt hensyn til i endelig rapport i den grad BDO og Wiersholm har funnet det riktig og nødvendig. Det er løpende tatt inn henvisninger til bemerkninger i fotnoter der dette har vært naturlig.

For øvrig har det vært jevnlig kontakt mellom NAV, BDO og Wiersholm, hovedsakelig i form av fremdriftsoppdateringer eller spørsmål som NAV som oppdragsgiver skal ta stilling til, jf. Advokatforeningens retningslinjer for private granskninger.

2.4.2 Dokumentasjonsinnsamling og dokumentgjennomgang

NAV har overlevert relevant dokumentasjon, herunder aktuelle rutiner, instrukser, rapporter og øvrig dokumentasjon. De ansatte BDO og Wiersholm har intervjuet har blitt oppfordret til å dele dokumentasjon som kan ha relevans for gjennomgangen.

Dokumentasjon er løpende lagret i en eDiscovery-plattform i henhold til gjeldende regelverk. Informasjonsdeling av personopplysninger mellom NAV, BDO og Wiersholm

har funnet sted ved at alle relevante prosjektmedarbeidere hos BDO og Wiersholm har hatt tilgang til dokumenter lagret i nevnte plattform, ved bruk av en sikker FTP-server eller ved bruk av filer med passordbeskyttelse sendt per epost. Fysisk dokumentasjon har blitt oppbevart på sikker måte. Videre vil personopplysninger bli slettet når formålet med behandlingen har opphørt. For øvrig lagres dokumentasjon i henhold til gjeldende regler for arkivering.

2.4.3 Intervjuer

BDO og Wiersholm har intervjuet til sammen ca. 60 personer. Dette inkluderer personer på alle nivåer i NAV samt enkelte personer ansatt i Arbeids- og velferdsdirektoratet.

Alle som har vært intervjuet har fått informasjon i forkant av intervjuene og har blitt gjort kjent med at informasjonen fra intervjuene vil kunne bli benyttet i forbindelse med rapporteringen til oppdragsgiver.

2.4.4 Sikkerhetsrevisjon

Som ledd av gjennomgangen er det gjennomført en sikkerhetsrevisjon. Formålet med sikkerhetsrevisjonen har vært å vurdere i hvilken grad NAVs styringssystem ivaretar rettslige krav, etterleves i praksis, og hvorvidt kravene fungerer etter sin hensikt. Det ble i forbindelse med gjennomføringen utarbeidet revisjonskriterier for å gi et normativt grunnlag for vurdering av avvik og forbedringspotensialer. NAV har valgt å etablere sitt styringssystem basert på standarden ISO 27001:2013 *Ledelsessystem for Informasjonssikkerhet*. Revisjonskriteriene er derfor basert på denne standarden, samt personopplysningsloven, personopplysningsforskriften og eForvaltningsforskriften. Funnene fra revisjonen og vurderingen av etterlevelse er innarbeidet i denne rapporten.

2.4.5 Spørreundersøkelse

For å kartlegge tilgangskontrollen i NAV, herunder om omfanget og karakteren av oppslag uten tjenstlig behov, er det utarbeidet en anonym spørreundersøkelse. Undersøkelsen inneholdt spørsmål rundt oppslag uten tjenstlig behov, håndhevingsregime, logging av oppslag, avvikshåndtering, samt opplæring og kjennskap til internt regelverk i NAV. I tillegg inneholdt undersøkelsen spørsmål om potensielle virkemidler for å forebygge oppslag uten tjenstlig behov.

Spørreundersøkelsen ble bearbeidet i samarbeid med Ressursgruppen. Undersøkelsen er gjennomgått og kvalitetssikret av IPSOS MMI AS. Spørreundersøkelsen ble først distribuert til 18 ansatte som var et utvalg testrespondenter. Spørreundersøkelsen ble deretter bearbeidet blant annet basert på tilbakemeldinger fra testrespondentene.

Endelig versjon av Spørreundersøkelsen ble distribuert til samtlige 20 958 ansatte i NAV. Totalt 8 474, tilsvarende ca. 40 %, besvarte spørreundersøkelsen i sin helhet. Besvarelsene er analysert av BDO og Wiersholm[4]. Ekspertise fra selskapet IPSOS MMI AS har bistått i dette arbeidet.

2.4.6 Logganalyse

BDO og Wiersholm har gjennomført analyser av loggdata fra Bisys, Gosys, Infotrygd, Joark, Modia, Personkortet og Pesys. Det er innhentet logginformasjon fra februar og april 2016 og det er kun data fra disse månedene som danner grunnlaget for resultatene fra logganalysen i denne rapporten.

Det ble, i samarbeid med Sikkerhetsseksjonen, identifisert flere mulige analyser for å identifisere omfang av enkelte typer av uautorisert bruk. Disse analysene ble identifisert på bakgrunn av hypoteser samt tidligere funn i utredninger gjennomført av

[4] Kun fullførte besvarelser er tatt med i analysene.

Internrevisjonen. Analysene som ble gjennomført undersøkte blant annet omfanget av oppslag på seg selv, oppslag på relasjoner, oppslag på kolleger i samme enhet og oppslag på brukere med geografisk nærhet til den som gjorde oppslaget.

Wiersholm har vurdert det rettslige grunnlaget for de logganalyser som var planlagt gjennomført, samt hvorvidt NAV hadde andre plikter ovenfor de ansatte, brukere eller andre, som måtte overholdes før analysene kunne påbegynnes. Oppsummert er det Wiersholms vurdering at NAV, og dermed BDO og Wiersholm, har hjemmel for å gjennomføre logganalysene etter både arbeidsmiljøloven og personopplysningsregelverket.

Det fullstendige datagrunnlaget besto av ca. 32 millioner logglinjer. Etter fratrekk av duplikater og andre irrelevante logglinjer,[5] besto datagrunnlaget av ca. 26 millioner oppslag gjort av ca. 18 000 medarbeidere.

Mulige feilkilder er forsøkt hensyntatt gjennom dialog og drøftelser med Sikkerhetsseksjonen og Kontrollansvarlige, samt validering av data med oppslag i NAVs eget loggsystem.

[5] Tilhørende slettede identer og alias-identer.

DEL 2 OM NAV

3. ORGANISERING

NAV ledes av Arbeids- og velferdsdirektoratet. Arbeids- og velferdsdirektøren[6] leder direktoratet, etaten og NAV-forvaltningen som sådan. NAV har ansvaret for gjennomføringen av arbeidsmarkeds-, trygde- og pensjonspolitikken, og skal forvalte arbeidsmarkedsloven, folketrygdloven (med unntak av kapittel 5) og andre lover hvor oppgaver er lagt til etaten, jf. lov om arbeids- og velferdsforvaltningen ("**NAV-loven**") § 4. I tillegg skal etaten overholde de krav som stilles i forvaltningsloven, personopplysningsloven, arkivregelverket og offentleglova, med tilhørende forskrifter.

Etaten skal bidra til å skape et inkluderende samfunn, et inkluderende arbeidsliv og et velfungerende arbeidsmarked i Norge. Etaten skal ivareta vanskeligstilte gruppers behov og bekjempe fattigdom, blant annet ved å stimulere til arbeid og deltakelse. Etaten har også ansvar for å sikre inntekt ved arbeidsløshet, svangerskap og fødsel, aleneomsorg for barn, sykdom og skade, uførhet, alderdom og dødsfall. Etaten ble opprettet ved den såkalte "NAV-reformen" i 2006 og består av en sammenslåing av tidligere Trygdeetaten og Arbeidsmarkedsetaten (Aetat).

NAV er en landsdekkende offentlig virksomhet som omfatter blant annet Arbeids- og velferdsdirektoratet, en arbeids- og tjenestelinje med lokale NAV-kontor i kommunene, en ytelseslinje og en økonomilinje. NAV har ca. 20 000 medarbeidere. Av disse er ca. 15 000 ansatt i Staten (NAV) og ca. 5 000 er ansatt i kommunene. På NAV-kontorene arbeider både statlig og kommunalt ansatte sammen.

Arbeids- og tjenestelinjen er satt sammen av blant annet NAVs fylkesledd, den statlige delen av NAV-kontorene, NAV Kontaktsenter og NAV Hjelpemidler og tilrettelegging. Linjen ledes av arbeids- og tjenestedirektøren i Arbeids- og velferdsdirektoratet.

Ytelseslinjen er delt inn i resultatområder med svært ulike ansvarsfelt. Tjenester og funksjoner som kan utføres regionalt og nasjonalt er samlet her. Hvert resultatområde blir ledet av en direktør som rapporterer til ytelsesdirektør i Arbeids- og velferdsdirektoratet. Enhetene i ytelseslinjen er organisert som nasjonale enheter - med regionale og fylkesvise kontorer - som løser oppgaver fra hele landet. Oppgavene enhetene gjør, frigjør tid ved NAV-kontoret til å følge opp brukere.

Hovedoppgavene til økonomilinjen er å sørge for at riktig utbetaling til brukere skjer til riktig tid og til riktig kontonummer, og at etatens samlede regnskap avlegges i tråd med økonomireglementet.

Arbeids- og velferdsdirektoratet har det overordnede ansvaret for at arbeids- og velferdsforvaltningen oppfyller de forventninger som stilles til etaten og når de mål og resultater som fremgår av Arbeids- og sosialdepartementets oppdrag. Direktoratet har ansvar for overordnet styring, ledelse og utvikling av NAV.

De tre styringslinjene i etaten - tjeneste-, ytelses- og økonomilinjen - har hovedansvaret for å gjennomføre arbeidet mot NAVs brukere. Styringslinjene ledes og styres av Tjeneste-, Ytelses-, og Økonomiavdelingen. I tillegg til disse avdelingene består etaten av fem andre avdelinger som koordinerer, legger rammer og fungerer som støttefunksjoner på tvers av linjer, herunder IKT-avdelingen. NAV har også en Internrevisjon som rapporterer direkte til arbeids- og velferdsdirektøren.

[6] Sigrun Vågeng tiltrådte som arbeids- og velferdsdirektør i 2015.

4. SAKSBEHANDLINGSKRAV

4.1 Krav til behandling av personopplysninger

NAV forvalter personopplysninger relatert til de fleste innbyggere i Norge. Behandling av personopplysninger utgjør en vesentlig og sentral del av NAVs kjernevirksomhet. Personopplysningsloven inneholder regler for behandling av alminnelige og sensitive personopplysninger. Betydelige mengder av personopplysninger knyttet til NAVs brukere er sensitive. Det behandles i tillegg betydelige mengder personopplysninger hvor konfidensialitet er nødvendig, herunder informasjon om personer som lever under særskilt beskyttelse klassifisert som brukere under kode 6 og 7[7]. NAV er avhengig av personopplysningene for å kunne sikre en korrekt forvaltning av velferdsordningene i Norge. Brukerne må kunne forvente at personopplysningene og annen taushetsbelagt[8] informasjon behandles forsvarlig og i henhold til lov, forskrift og internasjonale standarder. For å beskytte brukere og medarbeidere, og for å redusere risikoen forbundet med informasjonsbehandling, er det sentralt at sikkerhet har høy prioritet i NAV.

De norske reglene om personvern er forankret i Den europeiske menneskerettighetskonvensjonen og Grunnloven § 102. De konkrete prinsipper og regler er nedfelt i personopplysningsloven som suppleres av forskrifter[9]. Alle virksomheter i Norge har et selvstendig ansvar for å etterleve relevante personvernsrettslige regler og prinsipper. Dette er i økende grad en forpliktelse som tillegges den enkelte aktør. Forpliktelsene vil forsterkes ytterligere ved den nært forestående implementeringen av EUs nye personvernforordning i norsk rett.

Med personopplysning menes opplysninger og vurderinger som kan knyttes til en enkeltperson. Personopplysninger om blant annet helseforhold, seksuelle forhold og etnisk bakgrunn er å betegne som sensitive. Behandling av personopplysninger omfatter enhver bruk av personopplysninger, herunder innsamling, lagring og utlevering. Enkeltstående søk på personopplysninger i et informasjonssystem er også omfattet.

Regelverket fastsetter flere grunnleggende prinsipper, blant annet knyttet til konfidensialitet, integritet og tilgjengelighet, herunder formålsavgrenset bruk. Hensynet til konfidensialitet innebærer at opplysningene ikke skal gjøres tilgjengelige for uautorisert innsyn. Hensynet til integritet innebærer at opplysningene ikke skal kunne endres på uautorisert måte. Hensynet til tilgjengelighet innebærer at opplysningene skal være tilgjengelige og operative for autorisert bruk. Videre inneholder regelverket et grunnkrav til formålsavgrenset bruk av personopplysninger, samt krav til internkontroll, herunder at virksomheter skal etablere planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av loven.

I tillegg til å treffe tiltak som begrenser uautoriserte innsyn, skal det etter personvernlovgivningen iverksettes tiltak som gjør det mulig å oppdage og registrere forsøk på oppslag der det ikke foreligger noe tjenstlig behov.

Personopplysningsloven § 11 oppstiller grunnkrav til behandling av personopplysninger. Behandlingen skal kun skje når dette er tillatt etter personopplysningsloven §§ 8 (alminnelige personopplysninger) og 9 (sensitive personopplysninger), og i henhold til en fastsatt formålsavgrensning.

---

[7] Adressesperre som beskyttelsestiltak for trusselutsatte personer. Kode 7 innebærer at vedkommendes adresse ikke skal utgis til private, mens kode 6, som er den strengeste graden av beskyttelse, innebærer at opplysninger om vedkommendes adresse i utgangspunktet ikke skal gis ut til noen.

[8] Personopplysninger om brukere den enkelte har kjennskap til skal bevares konfidensielt. Ansatte signerer taushetserklæring ved ansettelse.

[9] Personopplysningsloven er den norske implementeringen av EUs personverndirektiv (Direktiv 95/46/EF) av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

Kravet til formålsavgrenset bruk innebærer for det første at den behandlingsansvarlige må fastsette et tilstrekkelig konkret og avgrenset formål om hva behandlingen skal tjene til.[10] Formålet skal være saklig begrunnet i behandlingsansvarliges virksomhet. For det andre må ikke personopplysningene senere brukes til formål uforenlige med det opprinnelige.[11] For det tredje må personopplysningene være tilstrekkelige og relevante for formålet med behandlingen.[12] Dette innebærer at opplysningsgrunnlaget må være så fullstendig som behandlingsformålet krever, uten at behandlingen omfatter unødvendige personopplysninger.[13]

I tillegg angir bestemmelsen at personopplysningene skal være korrekte og oppdaterte, og ikke lagret lenger enn nødvendig.[14] Dette kravet må ses i sammenheng med lovens krav til retting og lagring. Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige enten av eget tiltak eller etter begjæring fra den registrerte, rette de mangelfulle opplysningene.[15] Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger[16].

I april 2016 vedtok EU-parlamentet en ny personvernforordning. Forordningen vil erstatte dagens europeiske personvernregler, som bygger på EUs personverndirektiv av 24. oktober 1995, og som personopplysningsloven gjennomfører i norsk rett. Forordningen trer i kraft 25. mai 2018 og innebærer at alle EU land får ny, felles personvernlovgivning. Forordningen må også implementeres i Norge, som EØS-land. Det pågår for tiden forhandlinger mellom EØS-komiteen og EU. Forordningen omfatter mer enn dagens personvernregelverk i Norge, og det innføres en rekke nye plikter for virksomheter som behandler personopplysninger. Av særlig interesse for NAV er det at offentlige virksomheter pålegges å etablere personvernombud.

4.2 Krav til informasjonssikkerhet og internkontroll

Personopplysningsloven stiller krav om at den som behandler personopplysninger skal sørge for tilfredsstillende informasjonssikkerhet.[17] Kravet gir anvisning på at en risikoanalyse hvor truslene opplysningene er utsatt for og de konsekvenser en realisering av trusselen vil medføre, må kartlegges og vurderes. På bakgrunn av risikovurderingen skal virksomheten fastlegge kriterier for akseptabel risiko forbundet med behandlingen.[18] Nærmere bestemmelser om informasjonssikkerhet er gitt i personopplysningsforskriftens kapittel to som blant annet inneholder krav om sikkerhetsledelse, risikovurdering, sikkerhetsrevisjon, avvik, organisering, fysisk sikring, sikring av konfidensialitet, sikkerhetstiltak og sikkerhet hos andre virksomheter.

Personopplysningsloven § 13 (1) pålegger behandlingsansvarlig å etablere og gjennomføre planlagte og systematiske tiltak som skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet.

At tiltakene som gjennomføres skal være planlagte og systematiske innebærer at disse i utgangspunktet må foreligge før behandlingen tar til, at tiltakene skal følge en bestemt

---

[10] Ot.prp. nr. 92 (1998-1999) s. 113-114.

[11] Personopplysningsloven § 11 (1) bokstav c.

[12] Personopplysningsloven § 11 (1) bokstav d.

[13] Ot.prp. nr. 92 (1998-1999) s. 114.

[14] Personopplysningsloven § 11 (1) bokstav e.

[15] Personopplysningsloven § 27.

[16] Dersom tungtveiende personvernhensyn tilsier det, kan Datatilsynet, uten hinder av kravet om markering, bestemme at retting skal skje ved at opplysningene slettes eller sperres. Hvis opplysningene ikke kan kasseres i medhold av arkivloven, skal Riksarkivaren høres før det treffes vedtak om sletting. Vedtaket går foran reglene i arkivloven §§ 9 og 18.

[17] Personopplysningsloven § 13.

[18] Personopplysningsforskriften § 2-4.

metodikk og ikke være tilfeldige.[19] Det ligger i dette at behandlingsansvarlig må føre kontroll med hvem som har tilgang til personopplysningene som behandles. Tilsvarende må behandlingsansvarlig iverksette tilstrekkelige tiltak for å sikre at ansatte kun har tilgang til det som er nødvendig for å utføre den enkeltes arbeidsoppgaver. Personopplysningslovens regler legger dermed føringer for NAV-ansattes tilgang til og bruk av de ulike informasjonssystemene (tilgangsstyring), herunder at oppslag i informasjonssystemene gjøres i tråd med prinsippet om tjenstlig behov.

Personopplysningsloven § 14 og personopplysningsforskriften kapittel 3 stiller krav til internkontroll. Internkontrollen skal sørge for at informasjonssikkerheten og øvrige krav i personopplysningsloven sikres gjennom dokumenterte, planlagte og systematiske tiltak. Behandlingsansvarlig skal etter § 14 etablere og holde ved like de planlagte og systematiske tiltak som er nødvendige for å sikre oppfyllelse av kravene i eller i medhold av personopplysningsloven med forskrifter, eventuelle konsesjonsvedtak og andre enkeltvedtak fattet av Datatilsynet eller Personvernnemnda. Omfanget av de nødvendige tiltak avhenger av virksomhetens art, aktivitet og størrelse.[20]

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) har som formål å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon i forvaltningen. Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi).

Direktoratet for forvaltning og IKT (Difi) anbefaler at offentlige etater baserer seg på NS-ISO/IEC 27001:2013 ved etablering av styringssystem for informasjonssikkerhet. Hovedkravene består i at virksomheten skal implementere, vedlikeholde og forbedre eget styringssystem. Styringssystemet skal være forankret hos virksomhetens øverste ledelse, som skal sørge for at styringssystemet jevnlig gjennomgås for å sikre kontinuerlig forbedring av styringssystemet.

4.3 Øvrige krav til NAVs saksbehandling

Forvaltningsloven angir rammene for NAVs saksbehandling. Et grunnkrav i forvaltningsloven er at saksbehandlingen skal være forsvarlig. Kravet til forsvarlig saksbehandling blir ivaretatt gjennom lovens regler om habilitet, taushetsplikt, innsyn og informasjon.

Forvaltningsloven § 6 stiller krav om at offentlige tjenestemenn ikke skal treffe avgjørelse i en forvaltningssak eller tilrettelegge grunnlaget for slik avgjørelse hvor vedkommende er å anse som inhabil. Også forberedelse av forvaltningsvedtak er omfattet av habilitetsreglene. Automatisk inhabilitet foreligger blant annet hvor den ansatte selv er part i saken, har et tilstrekkelig nært slektskapsforhold og svogerskap til en part, er eller har vært gift med en part.[21] Videre vil den ansatte i NAV være inhabil dersom det foreligger *"særegne forhold"* som er egnet til å *"svekke tilliten til hans upartiskhet"*. Alternativet tar sikte på å fange opp de tilfeller som faller utenfor oppregningen i første ledd.

Offentlighetsloven skal legge til rette for innsyn og åpenhet i den offentlige forvaltningen.[22] Formålet er å legge til rette for videre bruk av slik informasjon. Etter loven gis enhver person rett til innsyn i saksdokumenter, journaler og lignende register, hvis ikke annet følger av lov eller forskrift. Et viktig unntak fra innsynsretten gjelder

---

[19] Personopplysningsloven §§ 31 (2) og 32 (1) bokstav i.

[20] Nærmere bestemmelser om internkontroll etter personopplysningsloven er gitt i personopplysningsforskriften § 3-1. eForvaltningsforskriften § 15 stiller også krav om internkontroll for informasjonssikkerhet.

[21] Jf. forvaltningsloven § 6 (1).

[22] Jf. offentlighetsloven § 1.

opplysninger underlagt taushetsplikt. NAV vil dermed ikke ha noen plikt etter offentlighetsloven § 3 til å gi personopplysninger som er omfattet av taushetsplikten.

De alminnelige bestemmelser om taushetsplikt i forvaltningen følger av forvaltningsloven §§ 13 til 13 e. Taushetsplikten er en plikt for å hindre at andre får adgang eller kjennskap til det en i forbindelse med tjenesten eller arbeidet får vite om "*noens personlige forhold*". Dette vil typisk være opplysninger om slektskaps-, familie- og hjemforhold, fysisk og psykisk helse og følelsesliv. Av lovens § 13 (2) fremgår at fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted ikke regnes som personlige forhold. Den alminnelige taushetsplikt gjelder således ikke disse forhold, med mindre opplysningene røper klientforhold eller andre forhold som anses som personlige.

NAV-loven § 7 inneholder særskilte regler om taushetsplikt i NAV, som på enkelte punkter går videre enn den alminnelige forvaltningsrettslige taushetsplikten. Etter § 7 (1) gjelder taushetsplikten for NAV også for fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted.

Taushetsplikten er ikke til hinder for at taushetsbelagte opplysninger brukes som ledd i saksbehandlingen.[23] Det kan derfor gis opplysninger til andre forvaltningsorganer når det er nødvendig for å fremme NAVs oppgaver.[24] Det følger videre av NAV-loven § 16 at taushetsplikten ikke er til hinder for at opplysninger er tilgjengelige for andre ansatte på kontoret i den utstrekning som trengs for en hensiktsmessig arbeids- og arkivordning, blant annet til bruk ved veiledning i andre saker. Dette til tross for at felles lokalkontor formelt sett omfatter to atskilte organer i forvaltningslovens forstand. Bestemmelsen innebærer at personopplysninger ved felles lokalkontor rettslig sett likestilles med organinterne opplysninger.[25]

Etter NAV-loven § 8 (2) skal etaten av eget tiltak gi sosialtjenesten opplysninger om forhold som kan føre til tiltak fra deres side. Slike opplysninger kan imidlertid bare gis etter samtykke fra brukeren eller med hjemmel i lov.

5. SIKKERHETSARBEIDET I NAV

5.1 Innledning

Arbeids- og velferdsdirektøren har det overordnede ansvaret for sikkerhet i etaten[26] og er dermed ansvarlig for de plikter som følger av loven og tilhørende forskrift. For kommunens del er behandlingsansvaret etter personopplysningsloven et ansvar som tilligger kommunen.[27] Det daglige ansvaret er delegert til lokal enhetsleder.[28] Regimeansvaret for personvern, informasjonssikkerhet og beredskap utøves av IKT-direktøren med støtte av seksjonssjefen for Sikkerhetsseksjonen, jf. punkt 5.2. IKT-direktøren har også ansvaret for sikkerhet i IKT-systemene samt for rutiner på sikkerhetsområdet, eksempelvis om tilgangskontroll, logging, sperringer og lignende.

Videre er det utpekt sikkerhetskoordinatorer ved enheter i direktoratet, fylkesleddet og i spesialenheter. Sikkerhetskoordinatorene skal bidra med kompetanse lokalt og koordinere sikkerhetsarbeidet, jf. punkt 5.3.

Den enkelte medarbeider har ansvar for å gjøre seg kjent med relevant sikkerhetsinformasjon, signere taushetserklæring, overholde taushetsplikten, sette seg

[23] Forvaltningsloven § 13 b (1) nr. 2.

[24] NAV-loven § 7(3).

[25] Ot.prp.nr. 47 (2005-2006).

[26] Jf. Styringsdokument for personvern, informasjonssikkerhet og beredskap, s. 7.

[27] Jf. Felles Sikkerhetsnormer, s. 4.

[28] Jf. Felles Sikkerhetsnormer, s. 4.

inn i og overholde etatens sikkerhetskrav som er relevante for medarbeiderens rolle i ulike situasjoner. Dette omfatter hva som er akseptabel bruk av informasjon og systemer, bruk av IKT-systemene som beskrevet i brukerdokumentasjonen samt krav til melding om avvik eller sikkerhetsbrudd eller ved mistanke om dette.[29]

5.2 Sikkerhetsseksjonen

Ansvaret for styringssystemet for personvern, informasjonssikkerhet og beredskap i NAV er lagt til IKT-avdelingen[30]. IKT-direktøren har delegert det daglige arbeidet med sikkerhet til seksjonssjef for sikkerhetsseksjonen i IKT-avdelingen. Seksjonssjef for Sikkerhetsseksjonen rapporterer kun til IKT-direktøren. Sikkerhetsseksjonen består p.t. av 10 ansatte, hvorav to jobber med personvern og resten med informasjonssikkerhet og beredskap. Sikkerhetsseksjonen er ansvarlig for etterlevelse av personopplysningsloven samt NAVs interne regelverk knyttet til personvern og informasjonssikkerhet. Sikkerhetsseksjonen forvalter retningslinjen *"Sikkerhetsgjennomgang i NAV"*. Retningslinjen benyttes av enhetsledere som innehar sikkerhetsansvaret på sin enhet og av sikkerhetskoordinatorer som bistår enhetsleder i dette arbeidet. Hensikten med sikkerhetsgjennomganger er å se at lover og regler etterleves og at etatens sikkerhetsnivå er tilfredsstillende.

Sikkerhetsseksjonen skal veilede, gi råd, overvåke helheten og gjennomføre nødvendige tiltak. Dette innebærer blant annet etterprøving og dokumentasjon av at sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer, gjennomføring av sikkerhetsbesøk på utvalgte enheter, utvikling av maler og verktøy samt formidle resultat av sikkerhetsgjennomganger til ledelsen i NAV.

5.3 Sikkerhetskoordinator og sikkerhetsmedarbeider

For å koordinere sikkerhetsarbeidet i de ulike enhetene kan det utpekes sikkerhetskoordinatorer i avdelingene i direktoratet, fylkeskontorene og i styringsenhetene[31]. Sikkerhetskoordinatorene kan blant annet bistå enhetslederen med å påse at egen og underlagte enheter følger sikkerhetsplan og pålagte krav, samt at tilgangskontroll og administrasjon av brukerprofiler til applikasjoner, servere og nettverk gis ut fra et tjenstlig behov. Sikkerhetsseksjonen fungerer som et faglig kontaktpunkt for sikkerhetskoordinatorene. Enhetsledere kan videre velge å utnevne en medarbeider til å arbeide med sikkerhet i egen enhet. Sikkerhetsmedarbeideren vil ha sikkerhetskoordinator i egen styringslinje som faglig støtteperson.[32]

5.4 Internrevisjonen

Ifølge Forskrift om internrevisjon i Arbeids- og velferdsetaten § 1 skal det etableres en internrevisjon. Internrevisjonen skal ha en uavhengig stilling og arbeide etter internasjonalt anerkjente standarder for internrevisjon. Revisjonsdirektøren rapporterer faglig og administrativt til arbeids- og velferdsdirektøren.

Internrevisjonen skal bistå NAV med revisjon og rådgivning for å oppnå strategiske mål. Gjennom risikobasert planlegging skal Internrevisjonen evaluere og bidra til forbedringer i virksomhetsstyring, risikostyring og internkontroll i all virksomhet i NAV i løpet av en 5-års syklus. Internrevisjonen avgir årlig en uttalelse om status på styring og kontroll i etaten.[33] Videre er Internrevisjonen etatens varslingskanal i henhold til varslingsrutine hjemlet i arbeidsmiljøloven § 3-6. Internrevisjonen er også ansvarlig for utredning av interne økonomiske misligheter. I forbindelse med dette arbeidet bistår Internrevisjonen

[29] Jf. Styringsdokument for personvern, informasjonssikkerhet og beredskap, s. 12.
[30] Styringsdokument for personvern, informasjonssikkerhet og beredskap, punkt 5.7.
[31] Styringsdokument for personvern, informasjonssikkerhet og beredskap, punkt 5.4.
[32] Styringsdokument for personvern, informasjonssikkerhet og beredskap, punkt 5.5.
[33] Årsrapport utarbeides i tillegg til tertialrapportering.

etaten med risikovurdering og læring i mislighetssaker. Internrevisjonen er også ansvarlig for å ivareta etatens rapporteringsplikt til Riksrevisjonen i mislighetssaker.

Internrevisjonen mottar hvert år tips som gjelder misbruk av tilgang til NAVs saksbehandlingssystemer. Alle mottatte tips skal følges opp. Saker som kun gjelder logginnsyn blir oversendt Sikkerhetsseksjonen som tar ut logger og forestår kommunikasjon med aktuelle enheter. Internrevisjonen blir koblet på i enkelte av sakene. Rapporter fra Internrevisjonens utredninger blir sendt til aktuelle ledere. Antall saker og funn blir oppsummert i Internrevisjonens årsrapport. I enkeltsaker utformes ikke konklusjoner, men vurderinger. Internrevisjonen anbefaler at personalansvarlig følger opp de aktuelle sakene. Det skal gis tilbakemelding til Internrevisjonen om eventuelle personalmessige konsekvenser. Behovet for et enhetlig reaksjonsmønster og en sentral oversikt over saker knyttet til misbruk av tilganger drøftes i kapittel 8.

6. TILGANG TIL OG BRUK AV FAGSYSTEMER

6.1 NAVs Fagsystemer

De fleste ansatte i NAV har behov for tilgang til personopplysninger om brukere for å utføre arbeidsoppgavene sine. Personopplysningene er tilgjengelige i NAVs saksbehandlingssystemer. De sentrale saksbehandlingssystemene for gjennomgangen er de som oftest benyttes av NAVs ansatte og som inneholder flest personopplysninger; Arena, Gosys, Pesys, Infotrygd, Bisys, Personkortet og Modia (de nevnte saksbehandlingssystemene omtales heretter som "**Fagsystemer**"). For å arbeide preventivt mot oppslag uten tjenstlig behov logges oppslag i disse Fagsystemene. Sikkerhetsseksjonen gjennomgår logger ved mistanke om uautoriserte oppslag, og har også tidligere forsøkt generell overvåkning basert på oversikter over medarbeidere med flest oppslag og brukere som er slått opp på flest ganger.

Arena er NAVs Fagsystem for oppfølgning av arbeidssøkere og forvaltning av ytelser under arbeidsledighet, arbeidsavklaring, og tiltaksdeltakelse. Arena benyttes også i oppfølgningen av sykemeldte og for saksbehandling knyttet til arbeidsgivere.

Gosys er et elektronisk registrerings- og oppgavefordelingssystem som skal understøtte arbeidsdelingen i etaten. Gosys benyttes derfor av mange ulike enheter og av svært mange ansatte i NAV. Elektronisk arkiverte dokumenter er tilgjengelige i dette Fagsystemet, eksempelvis alle medisinske opplysninger (sykemelding, legeerklæring, epikriser, etc.).

Pesys er NAVs Fagsystem for alderspensjon, uførepensjon (uføretrygd fra 1. januar 2015), AFP, gjenlevendepensjon, barnepensjon, krigspensjon, gammel yrkesskade og familiepleie.

Infotrygd er Fagsystemet som gir støtte til vedtak og utbetalinger for de fleste av saksområdene i tidligere Trygdeetaten. Systemet har et grensesnitt mot de fleste av NAVs systemer, og inneholder derfor store mengder personopplysninger.

Bisys er Fagsystemet for bidragssaker. Systemet kommuniserer direkte med de systemene som benyttes for innkreving og regnskapsføring av underholdsbidrag, og med de systemene som benyttes for utbetaling av bidrag.

Personkortet presenterer nøkkelinformasjon om en person hentet fra de viktigste Fagsystemene og kommunenes sosialsystemer. Det finnes kun lesetilgang i Personkortet, og det lagres ikke opplysninger i Personkortet.

Modia er en arbeidsflate som inneholder kjerneinformasjon om bruker og gir medarbeidere oversikt over brukerens saker, søknader og dialog med NAV. Modia henter informasjon fra flere Fagsystemer slik at dette samles på ett sted. Det lagres ikke personopplysninger i Modia.

6.2 Vilkår for tilgang til Fagsystemer

6.2.1 Innledning

Tilgang til de ulike Fagsystemene har betydning for hvilke personopplysninger NAVs ansatte kan få kjennskap til. Tilgang skjer gjennom tildeling av avgrensede roller til ansatte som varierer avhengig av en rekke faktorer. Tildeling av roller beror blant annet på type stilling den ansatte har, hvilket Fagsystem det gjelder, hvilken enhet vedkommende arbeider på, geografisk område, samt hvilke arbeidsoppgaver vedkommende har ansvar for. En ansatt vil ofte kunne ha flere roller i ett og samme Fagsystem for å kunne utføre sine daglige oppgaver. I Arena er det eksempelvis 23 ulike roller.

6.2.2 Tjenstlig behov

Personopplysningslovgivningen forutsetter at informasjonssystemer kun benyttes av autoriserte medarbeidere for utførelsen av pålagte oppgaver, og at det skal treffes tiltak for å hindre innsyn fra uautoriserte. NAV må dermed sørge for at den enkelte ansatte ikke gis tilgang til personopplysninger utover det som er nødvendig for at vedkommende skal kunne løse sine arbeidsoppgaver.

I NAV er det klare utgangspunktet for tilganger og roller i Fagsystemene at de skal være i henhold til "tjenstlig behov". Begrepet skal sammenfatte lovgivningens relevante krav til konfidensialitet, integritet og tilgjengelighet.[34] I motsetning til hva som er tilfelle i helse- og politisektoren, er ikke prinsippet for tilgangsstyringen nærmere presisert i lov.[35]

Ved anvendelse av normen skilles det ikke mellom behandling av sensitive personopplysninger og andre personopplysninger, herunder personopplysninger hvor konfidensialitet er tilsvarende nødvendig[36].

I praksis gir begrepet tjenstlig behov anvisning på to helt konkrete krav som stilles hver enkelt medarbeider i NAV. For det første innebærer dette at den enkelte ikke skal ha *tilgang* til mer enn vedkommende trenger for å gjøre sin jobb. For eksempel skal en saksbehandler i utgangspunktet ikke ha tilgang til Bisys dersom vedkommende ikke arbeider med bidragssaker. Samtidig vil informasjonen som er lagret om én bruker i ett Fagsystem kunne være relevant for en ansatt som til daglig arbeider med andre ytelser til samme bruker eller er veileder for denne.

For det annet ligger i begrepet et klart prinsipp om at ansatte i NAV ikke har lov til å gjøre *oppslag* i Fagsystemene de har tilgang til dersom det ikke er for å utføre en pålagt arbeidsoppgave. Dette gjelder selv om en ansatt faktisk har tilgang til et Fagsystem og informasjonen om brukere som fremgår der. Det vil eksempelvis ikke foreligge tjenstlig behov for å gjøre oppslag på seg selv eller på ens egen familie. I rollen som bruker har ansatte krav på innsyn i informasjon som er lagret om dem i NAVs Fagsystemer. Det er likevel ikke tillatt for ansatte selv å hente ut personopplysninger om seg selv i Fagsystemene.

Oppslag uten tjenstlig behov betegnes internt i NAV både som "uautoriserte oppslag", "uberettiget spørring" og "misbruk av tilgang", se kapittel 7 nedenfor. Ved innlogging i Fagsystemene må den ansatte identifisere seg med brukeridentitet og passord. Som

---

[34] I motsetning til hva som er tilfelle i helse- og politisektoren, er ikke dette prinsippet nærmere presisert i lovgivningen.

[35] Politiregisterloven § 21 slår fast at tjenestemenn i politiet og påtalemyndigheten bare kan gis tilgang til opplysninger dersom det foreligger et "tjenestemessig behov", og det formål opplysningene skal brukes til er omfattet av loven. Det følger av politiregisterforskriften § 8-3 at vilkåret er oppfylt dersom tjenestemannen vil settes i stand til å treffe en riktigere eller mer velbegrunnet avgjørelse, eller utføre en mer effektiv og hensiktsmessig tjeneste, enn om vedkommende ikke hadde hatt tilgang til opplysningene. Av helseregisterloven § 18 fremgår det at "(d)et er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven, uten særskilt hjemmel i lov eller forskrift". Sammenlignbare formuleringer er inntatt i pasientjournalloven § 16.

[36] I tråd med dette, og ut fra formålsbetraktninger har heller ikke BDO og Wiersholm i sitt arbeid opptegnet noe slikt skille mellom sensitive og ikke sensitive personopplysninger og personopplysninger hvor konfidensialitet er tilsvarende nødvendig.

følge av at oppslag i Fagsystemene i hovedsak logges, er det derfor i utgangspunktet mulig å avdekke misbruk av tilganger. Foretatte oppslag må i tilfelle vurderes opp mot den ansattes arbeidsoppgaver og tjenstlig behov.

6.2.3 Begrensninger i tilganger

Fagsystemene inneholder tekniske løsninger som i enkelte tilfeller begrenser muligheten for uautoriserte oppslag.

I praksis gis den enkelte ansatte tilgang til Fagsystemene gjennom tildeling av avgrensede roller. Den konkrete tildelingen beror blant annet på type stilling, hvilken enhet vedkommende arbeider på, geografisk område, samt konkrete arbeidsoppgaver den enkelte arbeidstaker er pålagt.

Ved ansettelse får samtlige medarbeidere i NAV tilbud om at det opprettes såkalt "ansattsperre" for vedkommende selv og dennes familie. Ansattsperren innebærer at det i utgangspunktet ikke kan gjøres oppslag i Fagsystemene på vedkommende eller dennes familie. Unntaket gjelder for ansatte som spesifikt er gitt slik tilgang ("tilgang til ansattfamilie"). Det er opplyst at ca. 3500 ansatte i NAV har tilgang til ansattfamilie. Disse behandler saker som knytter seg til andre ansatte i NAV og deres familier. Ansattsperre kan således i utgangspunktet hindre ansatte fra å gjøre oppslag på seg selv, familie og kolleger, forutsatt at vedkommende ansatt ikke har tilgang til ansattfamilie.

Tilgangene i enkelte av Fagsystemene kan gis permanent eller tidsbegrenset. Etter at en tidsbegrenset tilgang er utløpt, må vedkommende på ny gis tilgang dersom det fortsatt foreligger et tjenstlig behov for det. Tilganger vil også kunne være geografisk avgrenset, avhengig av hvilket Fagsystem det gjelder. Det kan eksempelvis gis enten lokal-, regional-, eller landsdekkende tilgang i Gosys. NAVs organisering innebærer at det er behov for vide geografiske tilganger. NAV Kontaktsenter er organisert slik at de ansatte besvarer henvendelser fra hele landet. De ansatte har dermed behov for landsdekkende tilgang til opplysninger om brukere for å kunne utføre sine arbeidsoppgaver.

For ansatte på lokale NAV-kontor vil det ikke bare være tjenstlig behov for lokal tilgang (bydel eller kommune). Dette skyldes blant annet at brukere arbeider og bor i ulike kommuner og oppsøker forskjellige NAV-kontor. Arbeidsmarkedet er heller ikke avgrenset av kommuner og regioner. Ofte får derfor ansatte på lokale NAV-kontor såkalt "utvidbar tilgang". Dette innebærer at de ved å oppgi en konkret begrunnelse for oppslag kan få tidsbegrenset utvidet tilgang utenfor bydelen eller kommunen. Begrunnelsen skal bekrefte at det foreligger tjenstlig behov for oppslaget. Det er ikke lagt tekniske føringer for hva begrunnelsen skal inneholde. Begrunnelsen medarbeideren oppgir loggføres slik at det kan kontrolleres om det forelå tjenstlig behov for oppslaget. Som nevnt i kapittel 5 gjennomgås imidlertid ikke loggene med mindre det foreligger mistanke om misbruk av tilgang.

Ved oppslag i Fagsystemene vil en ansatt kunne få tilgang til en rekke ulike personopplysninger, eksempelvis personnummer, adresse, sykemeldinger, epikriser og korrespondanse med leger. Forskjellige roller i Fagsystemene innebærer blant annet at det kan skilles mellom lese- og skrivetilgang. Dermed vil antallet ansatte som kan foreta andre handlinger enn å lese informasjonen kunne begrenses. Tilsvarende kan lesetilgangen for enkelte dokumenttyper forutsette at vedkommende ansatt innehar en spesifikk rolle, eksempelvis "Saksbehandler sensitiv tilgang" eller "Saksbehandler medisinsk tilgang". På denne måten kan også muligheten for at ansatte leser informasjon de ikke har tjenstlig behov for begrenses.

Det er kun et fåtall ansatte i NAV som har tilgang til personopplysninger om personer med fortrolig eller strengt fortrolig adresse (kode 6 og 7). Slike personopplysninger er

sperret for andre ansatte. Tildeling av tilgang til kode 6 og 7 følger særskilte rutiner og må godkjennes av Sikkerhetsseksjonen.

6.3 Nærmere om tilgangskontroll

I henhold til personopplysningsloven § 13 skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og de sikkerhetstiltak som etableres. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige, samt for Datatilsynet og Personvernnemnda. Formålet med dokumentasjonen er å bidra til at sikkerhetskravene etterleves i virksomheten.

I tillegg til å treffe tiltak som begrenser uautoriserte innsyn, skal det iverksettes tiltak som gjør det mulig å oppdage og registrere forsøk på slike oppslag. Lovgivningen stiller ikke konkrete krav til oppfyllelsen av dette, men det anbefales at det etableres systemer for logging i de Fagsystemene som benyttes. Dette omfatter tekniske logger for hvordan Fagsystemet brukes, herunder aktiviteten av vellykkede og mislykkede innloggingsforsøk, oppnådd adgang til filområder mv.

For å sikre styring og kontroll med hvem som får tilgang til Fagsystemene og for å hindre uautorisert innsyn i konfidensiell informasjon, er det etablert tilgangskontroll i NAVs Fagsystemer. I henhold til *"Overordnede Sikkerhetskrav"* skal tilgangskontrollen være presis, nøyaktig og mest mulig enhetlig. Den skal også administreres effektivt. Begrepet "tilgangskontroll" i vid forstand er i denne undersøkelsen tolket som å omfatte blant annet tilgangsstyring, sikkerhetsgjennomganger, logging av oppslag og avvikshåndtering. Tilgangskontroll utgjør dermed en sentral del av NAVs internkontroll med personvern og informasjonssikkerhet. Det er utarbeidet en rekke operative retningslinjer som skal sikre en tilfredsstillende tilgangskontroll, herunder retningslinjer som skal sikre etterlevelse av det interne regelverket.

For å sikre at etaten har god oversikt og kontroll over brukeridenter og den enkelte ansattes tilganger er det etablert retningslinjer for administrasjon av brukeridenter[37]. En "brukerident" er en personlig[38] identifikasjon ansatte benytter ved pålogging i NAVs informasjonssystemer. Både opprettelse, endring og sletting av brukeridenter skal foregå i henhold til etatens rutiner for dette. Administrasjon av roller i Fagsystemene følger ulike rutiner avhengig av hvilket Fagsystem det gjelder.

Medarbeidere skal som nevnt ha tilgang til det de trenger for å utføre sine arbeidsoppgaver. Enhetsleder er den nærmeste til å avgjøre behovet til sine medarbeidere. Enhetsleder er derfor ansvarlig for administrasjon av brukeridenter og tilgangsrettigheter til medarbeidere i egen enhet.[39] Dette skal sikre at tilgangene til enhver tid ikke er videre enn strengt nødvendig. Enhetsleder kan delegere arbeidet til en medarbeider i enheten som tildeles rollen som "identadministrator".[40] Ansvaret påhviler enhetsleder uavhengig av antall ansatte på enheten, men ved store enheter kan arbeidet delegeres til flere identadministratorer. Medarbeidere autoriseres først av enhetsleder. Deretter gir leder eller identadministrator teknisk tilgang og tildeler roller i Fagsystemene.

Videre er det enhetsleders ansvar å utøve løpende vedlikehold av tildelte rettigheter. Vedkommende er også ansvarlig for at det til enhver tid foreligger en dokumentert og oppdatert oversikt over brukeridenter i egen enhet, der godkjente tilganger per medarbeider fremgår.[41] Tilgangsstatistikker med antall som har utvalgte tilganger for

---

[37] "Brukeridenter og tilgangsrettigheter – rutiner for administrasjon".

[38] Både brukeridentitet og passord er personlig og skal ikke gjøres kjent for andre.

[39] Jf. "Dokumentasjon – Rollebeskrivelser fagsystemer", s. 3 samt "Brukeridenter og tilgangsrettigheter – rutiner for administrasjon", s. 4.

[40] Ibid.

[41] Det hender at rollen som sikkerhetskoordinator og rollen som identadministrator innehas av samme person.

hver enkelt enhet finnes også på Navet på siden "Tilgangskontroll". Oversikten skal gjennomgås jevnlig og minst én gang årlig av ledere med personalansvar. Formålet med gjennomgangen er å sikre at medarbeidere kun har tilganger på en "må vite" basis. Ved denne gjennomgangen skal brukeridenter som har vært inaktive i mer enn tre måneder inaktiveres. Dersom en medarbeider endrer arbeidsoppgaver, slutter eller av andre grunner har endret behov for tilganger skal enhetsleder og identadministrator umiddelbart følge opp.

Enkelte roller gir tilgang til veldig mye informasjon, mens andre roller gir tilgang til informasjon som krever høyere beskyttelsesnivå. Det er utarbeidet egne søknadsrutiner for å få tildelt tilganger i slike tilfeller. Dette gjelder eksempelvis landsdekkende tilgang i Infotrygd, landsdekkende tilgang i Personkortet samt brukere med skjermingskoder. Ansvar for behovsprøving av tilgang til sistnevnte gruppe er lagt til Sikkerhetsseksjonen.

DEL 3 PRAKTISK ETTERLEVELSE AV PERSONVERNLOVGIVNINGEN

7. OPPSLAG UTEN TJENSTLIG BEHOV – EKSISTENS OG OMFANG

7.1 Innledning

Sikkerhetsseksjonen har tidligere identifisert flere typetilfeller av oppslag uten tjenstlig behov. De viktigste typetilfellene er oppslag på seg selv, oppslag på relasjoner (familiemedlemmer), ved nyansettelser i NAV, samt oppslag på kolleger, bekjente eller offentlig kjente personer. Av motivasjonsfaktorer har Sikkerhetsseksjonen blant annet identifisert nysgjerrighet, undersøkelse eller påvirkning av en stønadssak samt opplæringsøyemed. Mange ansatte opplever lav eller ingen oppdagelsesrisiko knyttet til oppslag uten tjenstlig behov. Gjennomgangen har avdekket at de fleste ansatte ikke kjenner til om oppslag uten tjenstlig behov får personalmessige konsekvenser.

Gjennomgangen, herunder intervjuer, spørreundersøkelse og logganalyse, underbygger eksistensen av oppslag uten tjenstlig behov, og har også kartlagt omfanget i større utstrekning enn tidligere.

Ved besvarelsen av Spørreundersøkelsen har ca. 22 % opplyst at de har hørt om oppslag uten tjenstlig behov på enheten de arbeider eller har arbeidet i. Blant dem som har hørt om oppslag i Fagsystemene uten tjenstlige behov, er det forholdsvis få som har hørt om mange tilfeller. Det kan tyde på at det ikke er allment kjent at det er noen som gjør dette ofte. Tematikken kan til en viss grad være "tabu-belagt" fordi det er allment kjent i NAV at slike oppslag ikke er lov. 37 % av de som kjenner til slike oppslag opplyser at de har hørt om to til fem tilfeller. Det er oppslag på relasjoner, venner og på seg selv som nevnes hyppigst. Svarene fordeler seg på mange ulike kategorier, og viser et noe uklart mønster. Nysgjerrighet og egeninteresse oppgis hyppigst som årsaken til oppslag uten tjenstlige behov.

Basert på foreliggende informasjonskilder kan det konkluderes med at oppslag uten tjenstlig behov utgjør en utfordring for NAV. Denne type oppslag blir ikke fullt ut avdekket gjennom NAVs nåværende bruk av logginformasjon eller avviksrapportering. En virksomhet vil alltid kunne oppleve enkeltstående regelbrudd. Omfanget av uautorisert innsyn er av et større omfang enn NAV kan akseptere. Gjennomgangen har avdekket klare holdepunkter for at utfordringene er størst når det gjelder oppslag på seg selv, relasjoner og kolleger.

7.2 Oppslag på offentlig kjente personer

Spørreundersøkelsen avdekket at 22 % av respondentene som oppga kjennskap til uautoriserte oppslag, var kjent med oppslag på offentlig kjente personer. Enkeltsaker er også tidligere avdekket av Sikkerhetsseksjonen.

Logganalysene er benyttet for å kartlegge frekvensen av antall ansatte med oppslag på samme bruker. Antall ansatte med oppslag på samme bruker varierte fra 1 til 108.[42] Oppslag på samme bruker ble også analysert opp mot antall ulike enheter som hadde gjennomført oppslag. Antall enheter med oppslag på samme bruker varierte fra 1 til 30[43]. Tallene kan ikke isolert anses å utgjøre unormal aktivitet i Fagsystemene. Det vil være nødvendig å gjøre nærmere undersøkelser for å avklare om oppslagene var basert på tjenstlig behov. Det kan tenkes at det forelå tjenstlig behov dersom brukeren selv ofte har kontaktet NAV[44].

---

[42] I tillegg er det gjort 135 oppslag på én bruker som tilhører en testfamilie etablert for kontroll og testing av Fagsystemene.

[43] Med unntak av testbrukeren som det ble gjort oppslag på fra 73 ulike enheter.

[44] Brukere ringer inn til NAV Kontaktsenter som består av enheter over hele landet. Hvilken enhet som besvarer henvendelsen avhenger av kapasitet.

Logganalyser kan ikke isolert avdekke om det gjøres uautoriserte oppslag på offentlig kjente personer. Denne type loggdata gir imidlertid grunnlag for nærmere undersøkelser for å avklare eventuelt fravær av tjenstlig behov bak de enkelte oppslagene.

7.3 Oppslag på seg selv, relasjoner og kollegaer

Gjennomgangen har avdekket at ansattsperrer ikke benyttes i tilstrekkelig grad. Som nevnt i punkt 6.2.3, er det valgfritt om det skal opprettes ansattsperre ved ansettelse. Flere har opplyst at de ofte bruker seg selv eller kolleger i opplæringsøyemed eller som testbrukere. Funnene bekreftes av resultatene på spørreundersøkelsen, hvor både "testbruker" og "opplæring" hyppig ble oppgitt som begrunnelse for oppslag uten tjenstlig behov som de ansatte kjente til. Det var forholdsvis jevn fordeling av ansatte som hadde kjennskap til oppslag uten tjenstlig behov på relasjoner og på seg selv. Kjennskap til oppslag på kollegaer var noe lavere.

Til sammen ca. 12 % av alle medarbeidere som hadde gjort oppslag i februar og april har gjort ett eller flere oppslag på seg selv. Analysen viser at NAV har en utfordring med omfanget av ansatte som foretar oppslag på seg selv.

Antall oppslag på relasjoner ble funnet ved å sammenligne personnummeret det er gjort oppslag på og personnumrene til relasjonene til medarbeideren som gjorde oppslaget. Relasjoner er definert som barn, ektefelle/partner og foreldre. Denne analysen ble gjennomført på en populasjon bestående av ca. 12 500 medarbeidere. Ca. 11 % av disse har gjort oppslag på en eller flere relasjoner i løpet av februar og april.[45] I denne analysen ble det undersøkt hvor mange slike oppslag den enkelte hadde gjennomført i februar og april. Enkelte BDO og Wiersholm har intervjuet, har gitt uttrykk for at søk på relasjoner i enkelte tilfeller benyttes i opplærings- og testøyemed. Slike oppslag har uansett ikke tjenstlig behov.

Analyser av antall oppslag på medarbeidere i samme enhet som en selv (oppslag på kolleger) er kun gjennomført for medarbeidere på NAV-kontor. Denne avgrensingen er gjort for å forhindre "falske positive treff" på NAV-ansatte som bistår kolleger på tvers av regioner, som Brukerstøtte og NAV Forvaltning. Analysen kontrollerte oppslag hvor den som utførte oppslaget og den det ble gjort oppslag på har likt enhetsnummer. Oppslag på seg selv er ekskludert fra utvalget. Analysene viste at ca. 11 % har gjort oppslag på en eller flere medarbeidere i samme enhet. Tilsvarende som ved oppslag på relasjoner, har enkelte gitt uttrykk for at kolleger etter samtykke benyttes ved opplæring og tester.

7.4 Oppslag på bekjente

Et annet typetilfelle er oppslag på bekjente. Det kan forekomme tilfeller hvor ansatte har fått direkte forespørsel fra brukeren om eksempelvis å undersøke saksbehandlingen i en pågående stønadssak. Spørreundersøkelsen avdekket at ca. 26 % av respondentene med kjennskap til uautoriserte oppslag hadde kjennskap til oppslag på bekjente. Ca. 54 % trodde årsaken til oppslag uten tjenstlig behov skyldtes nysgjerrighet.

Det vil ikke gjennom rene logganalyser være mulig å undersøke om det forekommer uautoriserte oppslag på bekjente av en ansatt. Nærmere undersøkelser er i tilfelle nødvendig. Dette er en av årsakene til at slike oppslag ikke enkelt blir oppdaget uten konkret mistanke. Spørreundersøkelsen gir holdepunkter for at slike oppslag skjer, selv om dette ikke synes å ha like stort omfang som oppslag på seg selv, relasjoner og kolleger.

[45] Merk at flere av disse oppslagene er registrert på samme tidspunkt (på ulike relasjoner tilhørende samme person). Dette tilsier at oppslag på en relasjon i enkelte tilfeller genererer et "oversiktsbilde" over alle relasjoner, og at det dermed registreres loggoppslag på flere.

7.5 Oppslag ved ansettelser i NAV

Gjennom intervjuer har BDO og Wiersholm også blitt kjent med at det finnes tilfeller av oppslag i Fagsystemene på brukere som søker på ledige stillinger i NAV. Det er ikke tjenstlig behov for slike oppslag. Spørreundersøkelsen viste at dette var oppslag færrest ansatte hadde kjennskap til. Likevel var det 13 % av medarbeidere med kjennskap til uautoriserte oppslag som hadde kunnskap om oppslag på brukere ved ansettelser. Enkelte HR-ansatte har forklart at enhetsledere har etterspurt søkelister, foretatt oppslag i Fagsystemene og deretter henvendt seg til HR med anbefaling om ikke å ansette enkelte av søkerne. Fra sentralt hold er det opplyst at problematikken har vært tatt opp med lokale enhetsledere, men at utfordringen har vært tilbakevendende. Oppslag i forbindelse med nyansettelser vil ikke avdekkes ved enkle logganalyser med mindre det eksplisitt gjennomføres en kontroll hvor navn på jobbsøkere holdes opp mot brukere det er gjort oppslag på i perioden for ansettelse. Det må deretter gjøres nærmere undersøkelser av om det var tjenstlig behov for oppslaget.

8. BRUK AV LOGGER

Sikkerhetsseksjonen har adgang til å ta ut logger for oppslag i Fagsystemene. Dokumentet *"Retningslinje for bestilling og utlevering av logger"* regulerer bruk av logger. Det fremgår av dette dokumentet at loggene kun gjennomgås ved mistanke om uautorisert bruk.

Sikkerhetsseksjonen har i en 2-års periode overvåket logger for registrering av brukeraktiviteter og informasjonssikkerhetsbrudd. Ved slik overvåkning inngår brukere som har oppslag fra flest NAV-ansatte og medarbeidere med flest oppslag på hver enhet. Fra og med 2016 ble slik overvåkning av mønstre i logguttrekkene avsluttet. Etter dette har logger kun blitt gjennomgått ved mistanke om uautoriserte oppslag. Sikkerhetsseksjonen har bekreftet at det ikke gjennomføres generell overvåkning av loggene. Loggene benyttes følgelig ikke som preventivt tiltak for å forhindre oppslag uten tjenstlig behov eller som tiltak for å avdekke indikasjon på slike enkeltoppslag eller indikasjon på omfang av slike oppslag.

Rutiner og prosedyrer for logging av forsøk på uautorisert bruk av samtlige informasjonssystem i etaten mangler. Det mangler også rutiner for lagring av logger. Manglende rutiner for lagring av logger medfører risiko for at loggene blir slettet før det har gått tre måneder, jf. personopplysningsforskriften § 2-16 eller at opplysningene blir lagret lengre enn det som er nødvendig, jf. personopplysningsloven § 11 (1) bokstav e, jf. §§ 27 og 28. Det er avdekket at loggene lagres på ubestemt tid.

Gjennomgangen har avdekket at bruken av logger har vært fragmentert og mangelfull. Det vurderes som en svakhet at det ikke foreligger rutiner for regelmessig analyse av loggene, da dette er et viktig og lovpålagt virkemiddel for å sikre etterlevelse av det rettslige rammeverket[46]. De undersøkelser BDO og Wiersholm har utført ved hjelp av informasjon fra loggene har avdekket omfanget av brudd i gitte perioder. NAV sitter på informasjon som relativt enkelt danner grunnlaget for treffsikre undersøkelser som er velegnet til å avdekke misbruk av tilganger og oppslag uten tjenstlig behov.

9. REAKSJONSMØNSTER

9.1 Innledning

Som arbeidsgiver har NAV anledning til å benytte en rekke ulike reaksjoner overfor en ansatt som har gjennomført oppslag uten tjenstlige behov. Om personen er statlig eller

[46] Jf. personopplysningsforskriften § 2-14 (2). Bestemmelsen regulerer ikke bruk av logger, men hjemmel for dette kan utledes av personopplysningsloven § 14 jf. personopplysningsforskriften § 2-11 samt personopplysningsforskriften § 2-6.

kommunalt ansatt vil i noen grad ha betydning for hvilke krav som stilles til saksbehandlingen i det enkelte tilfellet.

Statlig NAV-ansatte er underlagt tjenestemannsloven. Kommunalt ansatte i NAV er underlagt arbeidsmiljølovens alminnelige bestemmelser. Dersom ansatte foretar oppslag i Fagsystemene uten tjenstlig behov, kan dette etter omstendighetene[47] gi grunnlag for tjenstlig tilrettevisning, ordensstraff, oppsigelse, avskjed og suspensjon; samt strafferettslige reaksjoner[48].

Et av hovedfunnene ved gjennomgangen er at NAV mangler oversikt over saker som gjelder oppslag uten tjenstlig behov. Videre mangler et enhetlig reaksjonsmønster overfor ansatte som foretar slike oppslag[49]. Spørreundersøkelsen avdekket at ca. 75 % av de ansatte ikke vet *om* ledelsen reagerer på oppslag uten tjenstlig behov. Når det gjelder kjennskap til ledelsens reaksjoner på oppslag uten tjenstlig behov er det utbredt mangel på kunnskap. Ca. 44 % av de som mener at ledelsen reagerer, vet ikke *hvordan* det reageres.

9.2 Manglende oversikt over saker

Et av funnene ved gjennomgangen er at NAV som sådan mangler en samlet oversikt over saker om oppslag uten tjenstlig behov samt hvordan NAV som arbeidsgiver har reagert i det enkelte tilfellet. Hvorvidt NAV, herunder Internrevisjonen, blir kjent med slike saker fremstår som noe vilkårlig. Andre avdelinger blir kun kjent med slike saker dersom det skjer i deres "linje".

Dersom en statlig ansatt er blitt ilagt en arbeidsrettslig reaksjon som går innunder tjenestemannsloven (ordensstraff, oppsigelse, avskjed) og påklager dette vedtaket, er Arbeidsgiverseksjonen sekretariat i saken, som behandles av det sentrale tilsettingsråd. I disse tilfellene får HR-avdelingen nødvendigvis kjennskap til saken. Etter det BDO og Wiersholm har fått opplyst, mottar det sentrale tilsettingsråd *maksimalt* et par saker i året som omhandler arbeidsrettslige reaksjoner som følge av oppslag uten tjenstlige behov.

NAV kan også bli kjent med enkeltsaker ved at HR-ansatte eller ledere i den enkelte driftsenhet henvender seg til Arbeidsgiverseksjonen for å få råd og veiledning i saker av denne typen i sitt fylke/resultatområde. Gjennomgangen har avdekket at viljen til å kontakte HR-avdelingen i slike tilfeller er varierende; enten fordi den enkelte enhet vil løse saken på egen hånd uten føringer fra sentralt hold, eller fordi den som utøver arbeidsgiveransvaret ikke anser at kontakten med Arbeidsgiverseksjonen gir noen merverdi i den aktuelle saken. Noen av intervjuobjektene har pekt på at et "silopreg" ved etatens organisering kommer tydelig frem i denne type saker.

Samlet sett er det klart at NAV mangler oversikt over hvor mange saker om oppslag uten tjenstlig behov som oppstår i NAV hvert år.

På grunn av manglende oversikt foreligger ikke presis kunnskap om i hvilke deler av etaten (geografisk eller faglig) hvor problematikken er mest aktuell. Dette vanskeliggjør en målrettet innsats på området.

---

[47] Valg av reaksjonsform avhenger blant annet av om vedkommende er statlig eller kommunalt ansatt.

[48] Jf. bl.a. TOSLO-2012-47498 og LB-2015-160098.

[49] Sveriges arbeids- og velferdsetater har tilsynelatende i større grad systematisert arbeidsrettslige reaksjoner overfor ansatte som foretar oppslag uten tjenstlig behov. Så vidt BDO og Wiersholm har forstått, har også etatene langt bedre oversikt enn NAV over slike saker og hvilke arbeidsrettslige reaksjoner de ansatte er blitt møtt med. Til illustrasjon behandlet Arbetsförmedlingens personalansvarsnämnd 17 saker i 2015 om uautorisert informasjonssøking. Nemda reagerte i 12 av sakene med advarsel. I de resterende fem sakene ble det ikke ilagt noen form for sanksjon. Försäkringskassans personalansvarsnämnd behandlet ni saker i 2015 som gjaldt uautorisert informasjonssøk. I 6 av overtredelsene reagerte nemnden med lønnstrekk, mens to saker resulterte i politianmeldelse. Én ansatt ble oppsagt. Kilde: Verksamhetsrapport för Arbetsförmedlingens personalansvarsnämnd (2015) punkt 3.1.1 og 3.5" samt "Forsikringskassens verksamhetsrapport PAN (2015)" (hele rapporten).

9.3 Manglende enhetlig reaksjonsregime

Gjennomgangen viser at NAV mangler et enhetlig reaksjonsregime for saker om oppslag uten tjenstlig behov. Dersom det oppdages at en ansatt har foretatt oppslag uten tjenstlig behov, er det den relevante enhetsleder som har det overordnede ansvaret for å vurdere om, og i tilfelle hva slags, arbeidsrettslig reaksjon den ansatte skal møtes med. Dersom personen er statlig ansatt, kan også det lokale tilsettingsråd måtte involveres, jf. tjenestemannsloven.

NAVs størrelse og sammensetning er en viktig forklaring på at reaksjonsmønsteret varierer noe. BDO og Wiersholm finner det klart er at praksisen varierer i for stor grad. Basert på Spørreundersøkelsen og gjennomførte intervjuer er det ikke grunnlag for å fastslå at praksis er basert på geografisk eller tjenestemessig tilhørighet, og dette ligger også utenfor mandatet. Det er likevel BDO og Wiersholms inntrykk at valg av reaksjon, og i så fall hvilken, i for stor grad er overlatt til den enkelte enhetsleders og/eller det enkelte tilsettingsråds skjønn. Resultatet av dette kan bli at like tilfeller kan bli underlagt ulik håndtering.

Manglende enhetlig reaksjonsregime kan utfordre ulovfestede saklighetsprinsipper, samt øke risikoen for at avvik og brudd ikke blir møtt med adekvate og korrekte sanksjoner. Følgelig er det også en risiko for at reaksjonsregimet ikke har den nødvendige preventive effekt, ettersom reaksjoner uteblir og varierer i alvorlighetsgrad.

10. STYRINGSSYSTEMET

10.1 Innledning

For å oppfylle personvernlovgivningens krav til behandling av personopplysninger og krav til informasjonssikkerhet må NAV ha et internt regelverk, jf. personopplysningsloven § 13. Regelverket må oppfylle lovens krav, vedlikeholdes, være tilgjengelig og kjent for ansatte. Retningslinjer, rutiner og instrukser har også til hensikt å sikre etterlevelse av relevante rettsregler. Etterlevelse sikres kun dersom regelverket er tilstrekkelig implementert i organisasjonen, blant annet gjennom opplæring. Opplæring og kjennskap til regelverket behandles i punkt 10.9. Brudd på plikter som følger av klare retningslinjer vil etter omstendighetene kunne sanksjoneres.[50] Følgelig har regelverkets utforming betydning for hvilke reaksjoner ansatte kan møtes med ved oppslag uten tjenstlig behov, jf. kapittel 8.

Arbeids- og velferdsetaten kan fastsette interne regler som gjelder for statlig ansatte i NAV. Tilsvarende gjelder når kommunalt ansatte behandler statlig informasjon eller benytter statlige Fagsystemer. I disse tilfellene er kommunalt ansatte også underlagt det statlige styringssystemet. For øvrig har ikke etaten myndighet til å pålegge kommunalt ansatte å følge etatens interne regelverk.[51]

Arbeids- og velferdsetaten har utarbeidet et omfattende sett med interne regler og retningslinjer for å ivareta de krav til informasjonssikkerhet og personvern. Etatens interne regelverk oppfyller i stor utstrekning de krav som følger av lovgivningen. I tillegg oppstilles en rekke mer detaljerte handlings- og unnlatelsesplikter i etatens rutiner og retningslinjer. Det interne regelverket er tilgjengelig for ansatte via intranettsiden "Navet".

For å oppfylle lovgivningens krav til informasjonssikkerhet[52] må NAV ha et styringssystem etablert på anerkjente standarder. Arbeids- og velferdsetatens interne styringssystem for

[50] Jf. eksempelvis Rt. 2001 s. 1589 og Rt. 2005 s. 518.

[51] BDO og Wiersholm har i henhold til mandatet ikke gjennomgått internt regelverk i den enkelte kommune. Etterlevelsen av lov- og forskriftspålagte krav er imidlertid vurdert for NAV som sådan.

[52] Se kapittel 4.

personvern, informasjonssikkerhet og beredskap er bygget opp i henhold til ISO 27001.[53] Styringssystemet består av dokumenter på tre nivåer. På det styrende nivået finnes *"Styringsdokument for personvern, informasjonssikkerhet og beredskap"* ("Styringsdokumentet"). Dokumentet *"Overordnede sikkerhetskrav"* er underordnet Styringsdokumentet. På gjennomførende nivå finnes *"Operativ sikkerhetsdokumentasjon"* som består av flere operative retningslinjer.

Dokumentene beskriver hvordan regimeansvaret for personvern, informasjonssikkerhet og beredskap er ivaretatt.[54] I tillegg benyttes ulike andre kilder til gode sikkerhetsnormer, som Information Security Forum (ISF) sin Standard of Good Practice (SoGP) for utdypning og rettesnor der dette er hensiktsmessig.[55]

"Ansvarsdokument for direktoratet" beskriver regime- og linjeansvaret i direktoratet. Ansvarsdokumentet beskriver direktoratets hovedansvar for virksomheten og direktørenes ansvar med hovedoppgaver for den enkelte avdeling og stab. Ansvarsdokumentet er premissgiver for direktoratets virksomhet sammen med øvrige styrende dokumenter. Dokumentet blir oppdatert når det skjer endringer i ansvarsforhold.[56]

Det er også utarbeidet et sett med *"Felles Sikkerhetsnormer"* som gjelder for *både* statlig og kommunal del av forvaltningen. Dokumentet skal sikre felles forståelse mellom stat og kommune med hensyn til sikkerhetsnivå ved felles lokalt kontor. Dokumentet inneholder konkretisering av lovmessige krav som alle enheter i Arbeids- og velferdsforvaltningen bør implementere.[57]

10.2 Overordnede Sikkerhetskrav

Dokumentet Overordnede sikkerhetskrav sammenfatter felles sikkerhetskrav innen områdene personvern, informasjonssikkerhet og beredskap som gjelder for etaten. Dokumentet ble sist oppdatert 17. februar 2015.

Dokumentet har fire vedlegg:

> *"A. Oversikt over relevante regelverk som NAV må forholde seg til innen sikkerhetsområdet*
>
> *B. Oversikt over operative retningslinjer som detaljerer kravene innenfor rammene av dette dokumentet*
>
> *C. Definisjoner over sentrale begreper som benyttes i sikkerhetsdokumentene*
>
> *D. Oversikt over de viktigste interessentene til sikkerhet i NAV"*

Punkt 1 gjelder personvern:

> *"NAV skal sikre personvernet gjennom en forsvarlig og sikker behandling av personopplysninger. En forsvarlig behandling vil bidra til korrekte avveininger og avgjørelser. Arbeidet med personvern og herunder overholdelse av taushetsplikt skal bidra til ivaretakelse av rettsikkerhet og konfidensialitet. Et godt personvern skal sikre at forvaltningens brukere og samfunnet for øvrig, har tillit til NAVs behandling av personopplysninger".*[58]

---

[53] Sikkerhet i NAV 2013, versjon 1.0, Grunnlag for ledelsens gjennomgang av personvern, informasjonssikkerhet og beredskap.

[54] Jf. Styringsdokument for personvern, informasjonssikkerhet og beredskap, s. 4.

[55] Ibid.

[56] Jf. Ansvarsdokument for direktoratet, versjon 1.5, forsiden.

[57] Jf. Felles Sikkerhetsnormer, forsiden. Det er opplyst at kommunale NAV-kontor i stor grad har implementert statlige rutiner og retningslinjer. Dette er imidlertid ikke kontrollert av BDO og Wiersholm.

[58] Ibid s. 8.

Videre følger det av punkt 1.3 "Brukers rettigheter" at NAV skal behandle personopplysninger innenfor definerte formål og lovlig rettsgrunnlag. Punkt 1.5 gjelder taushetsplikt som følger av arbeids- og velferdsforvaltningsloven, lov om sosiale ytelser i NAV og forvaltningsloven.

Dokumentet inneholder for øvrig krav til intern organisering av sikkerhet, herunder personellsikkerhet. Av punkt 4.2.2 om "Opplæring i sikkerhet og etablering av sikkerhetskultur" fremgår:

> *"Alle medarbeidere skal ha tilstrekkelig kompetanse om personopplysningsloven og personopplysningsforskriftens bestemmelser som er av betydning for deres arbeidsoppgaver.*
>
> *Alle medarbeidere skal ha kjennskap til informasjonssikkerhetskrav og prosedyrer som gjelder for sine oppgaver.*
>
> *[…]*
>
> *Det skal i tillegg til grunnleggende opplæring i de ulike sikkerhetsområdene gis regelmessig informasjon og nødvendig opplæring for å sikre at kunnskap om oppdaterte rutiner og krav og som en oppfriskning av den grunnleggende opplæringen.*
>
> *[…]*
>
> *Brudd på sikkerhetsbestemmelsene skal følges opp av nærmeste leder innenfor rammene av personalreglementet".*

Definisjonen av og virksomhetskrav til tilgangskontroll fremgår av punkt 6:

> *"Å styre og kontrollere tilgang til informasjon og informasjonssystemer for å hindre uautorisert tilgang og sikre autorisert tilgang."*
>
> *"Tilganger skal gis i henhold til prinsippet om tjenstlig behov. Medarbeidere skal kun gis de tilganger de trenger å ha for å gjøre sitt arbeid."*[59]

I henhold til punkt 6.2.5 skal *"alle ledere med personalansvar skal jevnlig foretas [sic] gjennomgang av at tildelte tilganger er i tråd med tjenstlig behov"*.

Kapittel 12 omhandler sikkerhetshendelser og avvik, herunder ansvar knyttet til avviksrapportering og håndtering av avviks- og sikkerhetshendelser samt læring og dokumentering av bevis:

> *"Alle medarbeidere er ansvarlige for å rapportere sikkerhetshendelser og avvik som de oppdager eller blir gjort kjent med til enhetsleder. Sikkerhetshendelser og avvik skal rapporteres så snart som mulig gjennom avviksrapporteringssystemet (ASYS)."*

Kapittel 15 som gjelder etterlevelse, fastsetter at Sikkerhetsseksjonen skal ajourholde oversikt over lover, forskrifter og kontraktsmessige forpliktelser som regulerer sikkerhetsområdet. Det er også Sikkerhetsseksjonen som er ansvarlig for å utarbeide operative retningslinjer.[60]

10.3 Felles Sikkerhetsnormer

Felles Sikkerhetsnormer inneholder generelle regler for sikkerhet i Arbeids- og velferdsforvaltningen (NAV). Reglene knytter seg til ansvar, opplæring og kompetanse,

[59] Jf. Overordnede Sikkerhetskrav, punkt 6.1.

[60] En oversikt over alle gjeldende operative retningslinjer finnes i Vedlegg B til Overordnede sikkerhetskrav.

lokal vs. sentral styring av sikkerhet og rapportering. Samtlige medarbeidere skal gjøres kjent med og undertegne Felles Sikkerhetsnormer, Appendiks A "Sikkerhetsinstruks for medarbeider". Instruksen gjelder uavhengig av om vedkommende er ansatt i stat eller kommune.

Instruksen inneholder detaljerte regler for informasjonshåndtering, herunder om håndtering av personopplysninger, lagring, dokumentforsendelser, elektronisk kommunikasjon, samt innsyn, utlevering og retting/sletting av informasjon. Instruksen fastsetter grunnleggende krav til behandling av personopplysninger i NAV under henvisning til personopplysningsloven:

> *"Personopplysningsloven gjelder helt fra det er registrert enkle opplysninger vedrørende en enkeltperson;*
>
> *Personopplysninger i forvaltningen skal ikke gjøres tilgjengelig for uautoriserte medarbeidere eller uvedkommende.*
>
> *Det skal ikke søkes etter opplysninger om personer som du ikke har bruk for i det daglige arbeid. Alle autoriserte oppslag skal ta utgangspunkt i om det foreligger et tjenstlig behov."*

Sikkerhetsinstruksen gjelder for alle typer oppgaver og funksjoner dersom det ikke foreligger annen avtale eller instruks. Eventuelle tilleggskrav skal dokumenteres lokalt.[61]

Enhetsledere med personalansvar er også forpliktet til å signere Tilleggsinstruks for leder, inntatt som Appendiks B til Felles Sikkerhetsnormer. Tilleggsinstruksen fastsetter blant annet at enhetsleder er ansvarlig for at taushetserklæring for NAV er lest og underskrevet før det gis tilgang til IKT-systemer, samt at alle medarbeidere er kjent med, og har satt seg inn i og signert sikkerhetsinstruksen.[62]

Videre skal leder sørge for at ingen medarbeidere gis tilgang til IKT-systemer eller informasjon ut over det som er helt nødvendig for å utføre pålagte arbeidsoppgaver (tjenstlig behov). Leder har også ansvar for å sørge for løpende vedlikehold av tildelte rettigheter til IKT-systemene, samt tilstrekkelig opplæring. I tillegg er leder ansvarlig for at alle medarbeidere har fått nødvendig tilgang til, og forståelse for, forvaltningens krav til personvern, informasjonssikkerhet og beredskap. Leder skal ved organiseringen av arbeidet og tildeling av oppgaver sørge for at det tas tilstrekkelig hensyn til personvern og taushetsplikt.[63]

10.4 Styringsdokumentet

Arbeids- og velferdsetatens styringsdokumentasjon for behandling av personopplysninger er nedfelt i dokumentet Styringsdokumentet, sist godkjent 17.februar 2015[64]. Styringsdokumentet inneholder de overordnede prinsipper og krav til sikkerhet i etaten. Dokumentet beskriver ansvarsforholdene for rutineoppfølgning i etaten, rammer, sikkerhetsmål, sikkerhetsstrategier samt policyområder som ligger til grunn for sikkerhetsarbeidet.

Det fremgår innledningsvis av kapittel 2[65] at det overordnede effektmålet er å bidra til å ivareta etatens "*allmenne tillit og rennommé*" og videre at grunnleggende krav til personvern skal ivaretas ved behandlingen av personopplysninger:

---

[61] Jf. Sikkerhetsinstruks for medarbeider, s. 6.

[62] Jf. Tilleggsinstruks for leder, s. 12.

[63] Ibid.

[64] Målene, strategiene og kravene i styringssystemet for personvern, informasjonssikkerhet og beredskap gjelder for den statlige delen av NAV, og kan også brukes av den kommunale delen.

[65] Jf. Ansvarsdokument for direktoratet, s. 5.

"Når vi behandler personopplysninger skal vi sikre grunnleggende krav til personvern ved å:

Etterleve våre plikter som behandlingsansvarlig. Det gjelder krav til gyldig behandlingsgrunnlag, vurdering av formål og sikre kvalitet ved behandling av personopplysninger, ivaretakelse av melde- og konsesjonsplikt.

Sikre brukers rettigheter etter personopplysningsloven. Det gjelder tilstrekkelig informasjon om behandlinger, ivaretakelse av informasjonsplikten, riktig håndtering av innsynsrettigheter, retting/sletting av mangelfulle personopplysninger.

Ha ekstra sterk fokus på personvern når vi behandler sensitive personopplysninger."

Direktørene for linjer og staber har linjeansvar for personvern og sikkerhet. Innenfor sikkerhetsområdet har direktørene bl.a. ansvar for å *"stille sikkerhetskrav til systemer, tjenester og informasjon innen eget fagområde. Herunder sikre at identitets- og tilgangshåndtering er basert på tjenstlig behov."*[66] Enhetsledere i linjen har ansvar for å *"etablere og opprettholde et tilstrekkelig sikkerhetsnivå innenfor sitt ansvarsområde, herunder påse at fagansvarlige, prosjektledere og medarbeidere i enheten har tilstrekkelig kunnskap, bevissthet og holdninger for personvern, informasjonssikkerhet og beredskap"*.[67]

Den enkelte medarbeider har ansvar for å gjøre seg kjent med relevant sikkerhetsinformasjon, signere taushetserklæring, overholde taushetsplikten, sette seg inn i og overholde etatens sikkerhetskrav som er relevante for medarbeiderens rolle i ulike situasjoner. Dette omfatter hva som er akseptabel bruk av informasjon og systemer, bruk av IKT-systemene som beskrevet i brukerdokumentasjonen samt melding om avvik eller sikkerhetsbrudd eller mistanke om dette.[68]

10.5 Operative retningslinjer

De operative retningslinjene gir detaljerte sikkerhetsregler med veiledninger og bindende rutinebeskrivelser på områder med behov for dette. Retningslinjene beskriver hvordan sikkerhetskrav utføres og etterleves i praktisk handling.[69] Retningslinjene utarbeides og oppdateres løpende av Sikkerhetsseksjonen innenfor rammene av Styringsdokumentet og Overordnede sikkerhetskrav.

I henhold til oversikten i Vedlegg B til Overordnede Sikkerhetskrav, foreligger det mer enn 55 operative retningslinjer for personvern, informasjonssikkerhet og beredskap. Retningslinjene er delt inn i 15 ulike fokusområder. De mest sentrale fokusområdene for gjennomgangen er *"Personvern og taushetsplikt"*, *"Tilgangskontroll"*, *"Sikker kommunikasjon"*, *"Håndtering av sikkerhetshendelser og -avvik"*, samt *"Etterlevelse av lover og regler"*.

NAV har også utviklet en veileder som gjelder gjennomgang av tilganger. Dokumentet har til formål å sikre etterlevelse av kravene i personopplysningsloven som gjelder kontroll på hvem som har tilgang til hva. I tillegg publiseres det jevnlig informasjon knyttet til temaene personvern og informasjonssikkerhet på intranettsiden Navet. Denne informasjon har til formål å påminne, lære opp og informere ansatte om kravene i de operative retningslinjene.

---

[66] Jf. Styringsdokument for personvern, informasjonssikkerhet og beredskap, s. 10.

[67] Ibid.

[68] Jf. Styringsdokument for personvern, informasjonssikkerhet og beredskap, s. 12.

[69] Overordnede sikkerhetskrav, Vedlegg B: Oversikt over operative sikkerhetskrav, s. 34.

10.6 Vurdering av styringssystemet

Styringssystemet for personvern, informasjonssikkerhet og beredskap består som skissert over av styringsdokumentasjon som gir overordnede føringer, oversikt over de sikkerhetskrav som gjelder for etaten, samt operative retningslinjer som skal gi detaljert veiledning for å sikre etterlevelse av sikkerhetskrav.

Arbeids- og velferdsetaten har i stor grad utarbeidet de nødvendige *styrende* dokumentene som skal inngå i et styringssystem, herunder *"Styringsdokument (Informasjonssikkerhetspolicy)"*. Ledelsen i NAV viser her eierskap til styringssystemet, og ansvaret for drift og vedlikehold av styringssystemet er godt beskrevet og forankret.

Det er utarbeidet mål for informasjonssikkerhet og personvern i den styrende dokumentasjonen, men flere av disse er ikke målbare. Hensikten med å måle styringssystemet er å sørge for kontinuerlig forbedring av prosessene, samt å sikre etterlevelse av krav i lov og forskrift og øvrige interne sikkerhetskrav. NAV risikerer derfor at virksomheten ikke er i stand til å sørge for at relevante lov- og forskriftskrav følges.

"Ledelsens gjennomgang" av personvern, informasjonssikkerhet og beredskap gir et godt bilde på hvilke risiki som vurderes mest vesentlig, samt resultater etter sikkerhetsgjennomganger. Gjennomgangen er likevel i liten grad koblet opp mot hvorvidt styringssystemet fungerer etter hensikten. Da tiltakene som foreslås i ledelsens gjennomgang ikke er koblet opp mot ytelsen til styringssystemet, vil det i praksis være løsrevet fra vurderingen av hvordan kravene til personvern, informasjonssikkerhet og beredskap etterleves. Det vises heller ikke at ledelsen drøfter i hvilken grad organiseringen og de ressursene som er avsatt til å drifte styringssystemet er fornuftige og tilstrekkelige.

Kjennskapen til mål og prioriteringer for informasjonssikkerhet og personvern er varierende i organisasjonen. Det mangler en tydelig kommunikasjon av hva som er etatens overordnede mål på området. Personvern er ikke omtalt i etatens overordnede strategidokumenter. Det vises i denne sammenheng til vår overordnete vurdering av manglende strategisk fokus på prioritering.

Dokumentasjonen for *"Helhetlig risikostyring på sikkerhetsområdet*" legger klare føringer for etatens kontinuerlige sikkerhetsarbeid, men det vurderes at risikostyringsprosessen likevel bør knyttes tettere opp mot styringssystemet enn det er i dag. Risikovurderinger skal danne grunnlaget for hvilke sikkerhetstiltak og overordnede sikkerhetsmål som skal prioriteres i organisasjonen. Da arbeids- og velferdsetaten mangler en anvendelighetserklæring[70], er det ikke påvist at dette gjøres.

Den *styrende* dokumentasjonen tilfredsstiller på de fleste punkter også personopplysningslovens krav. Det er likevel identifisert enkelte vesentlige avvik fra personopplysningsforskriftens kapittel 2, blant annet manglende kartlegging av hvilke typer personopplysninger som behandles, mangelfulle risikovurderinger, samt manglende beskrivelse av NAVs formål med behandling av personopplysninger i etatens sikkerhetsmål[71].

En rekke av arbeids- og velferdsetatens systemer mangler dokumenterte risikovurderinger. Det gjennomføres periodiske risikovurderinger, både overordnet og på lokale kontorer. Stikkprøver viser at de lokale risikovurderingene i liten grad vurderte risiko relatert til informasjonssikkerhet, og at de videre ikke i tilstrekkelig grad kartla

[70] Sikkerhetstiltakene skal etter ISO-standard 27001 sammenliknes med sikkerhetstiltakene i standardens vedlegg A – Relevante sikringstiltak for å håndtere risiko. Alle sikkerhetstiltakene i vedlegg A skal gjennomgås i en anvendelighetserklæring, og dersom tiltak ikke benyttes skal det begrunnes. Etaten har ikke utarbeidet en anvendelighetserklæring.

[71] Jf. personopplysningsloven § 2-4.

sannsynligheten for, og konsekvenser av sikkerhetsbrudd for hver enkelt behandling av personopplysninger.

Avvikene kan avhjelpes gjennom forbedringer av styringssystemet, jf. kapittel 11.

Arbeids- og velferdsetatens *styringsdokument* er konkretisert i Overordnede Sikkerhetskrav, som videre er operasjonalisert i 55 *operative retningslinjer* som skal ivareta kravene til internkontroll etter personopplysningsloven § 14, jf. personopplysningsforskriften § 3-1. Dette utgjør den *gjennomførende* dokumentasjonen i styringssystemet. Denne er svært omfattende og delvis overlappende. Det er ikke i strid med lovgivningen å ha mange interne regler, men det kan skape et hinder for etterlevelse i organisasjonen. Det kan være vanskelig for ansatte å navigere i all dokumentasjonen. Dette kan igjen medføre at retningslinjene ikke blir benyttet, eller at ansatte er usikre på hvilke retningslinjer som gjelder for dem og de arbeidsoppgavene vedkommende skal utføre. Tilsvarende kan et omfattende regelverk medføre uklarhet om den enkeltes ansvar og rolle. Viktige interne regler kan i verste fall "forsvinne" i mengden av dokumenter. Videre er det problematisk at prinsippet og kravet om tjenstlig behov er definert ulikt i flere av retningslinjene. Mange retningslinjer har også til dels overlappende navn. Dette kan bidra til forvirring[72].

Når omdømmemessige betraktninger fremheves som et overordnet effektmål, står det etter BDOs og Wiersholms oppfatning i fare for å overskygge viktigere formål nedfelt i den relevante personvernlovgivningen. Videre er det BDOs og Wiersholms vurdering at de operative retningslinjene er mangelfulle på enkelte områder, jf. personopplysningsloven § 3-1. Følgende rutiner er lovpålagt å ha dokumentert, og det er funnet at disse enten er mangelfulle eller mangler i sin helhet:

- Rutiner/interne retningslinjer for å sikre at personopplysninger ikke lagres lengre enn det som er nødvendig ut i fra formålet (sletterutiner). Det er ikke utarbeidet konkrete sletterutiner, herunder frister, for NAV. BDO og Wiersholm har fått opplyst at det pågår et arbeid for å etablere en felles bevarings- og kassasjonsplan for NAV. Konkretisering av slettefrister fremgår i dag av kassasjonsrutiner for AETAT og Trygdeetaten. Etter BDO og Wiersholms vurdering er disse sletterutinene mangelfulle. Det fremgår blant annet ikke når og hvordan «meropplysninger» skal slettes.
- Rutiner/interne retningslinjer for vurdering av formål med behandling av personopplysninger i samsvar med personopplysningsloven § 11 bokstav a er ikke mottatt. Det er behov for en konkret rutine som sikrer at formålet med behandling av personopplysninger samsvarer med det rettslige grunnlaget.
- Rutiner/interne retningslinjer for vurdering av personopplysningenes kvalitet for det definerte formålet med behandling av opplysningene, jf. personopplysningsloven §§ 11 bokstav d og e, 27 og 28, samt oppfølging av eventuelle avvik mangler. Det er behov for en konkret rutine som sikrer at mottatte personopplysninger er oppdaterte og tilstrekkelig ut fra formålet.
- Rutiner/interne retningslinjer for å sikre oppfyllelse av informasjonsplikt til de registrerte mangler.

10.7 Særlig om innebygd personvern

Innebygd personvern er ett av fire prinsipper i overordnet strategi for sikkerhetsarbeidet[73] i NAV. Strategien innebærer at systemer og prosesser skal utvikles etter prinsipper for

[72] I denne kontekst bør imidlertid også fremheves at en stor andel av respondentene i spørreundersøkelsen mente at de retningslinjer de er kjent med er enkle å forstå, se særlig pkt. 10.9 nedenfor.

[73] Styringsdokument for personvern, informasjonssikkerhet og beredskap (informasjonssikkerhetspolicy).

innebygd personvern.[74] Innebygd personvern er ikke et krav etter personopplysningsloven eller personopplysningsforskriften. EUs personvernforordning[75] inneholder imidlertid bestemmelser som pålegger virksomheter å etablere tilfredsstillende tekniske og organisatoriske sikkerhetstiltak. Dette gjelder både ved utvikling og etablering av informasjonssystem og før oppstart av selve behandlingen av personopplysninger.

Innebygd personvern i arbeids- og velferdsetaten er operasjonalisert gjennom *Retningslinjer for Sikkerhet ved anskaffelse, utvikling og forvaltning av IKT-systemer*. Retningslinjene skal bidra til å sikre at utviklings- og anskaffelsesprosjekter ivaretar sikkerhets- og personvernhensyn fra start og gjennom prosjektfasene. I tillegg er det utarbeidet en liste over ikke-funksjonelle krav knyttet til systemutvikling og vedlikehold. I de ikke-funksjonelle kravene inngår blant annet en rekke krav om pålitelighet og sikkerhet som systemene skal oppfylle. Hensikten med kravene er å være en form for sjekkliste som skal gjennomgås internt og med eventuelle leverandører under utviklingsfasen, og før implementering av nye systemer.[76] De omtaler i hovedsak anskaffelse av nye systemer, eller vedlikehold av systemer som allerede har elementer av sikkerhet innebygget.

10.8 Håndtering av avvik

Etter personopplysningsforskriften § 2-5 (1) har den behandlingsansvarlige plikt til å gjennomføre en jevnlig sikkerhetsrevisjon av bruken av informasjonssystemet. Sikkerhetsrevisjonen skal blant annet inneholde en vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom det blir avdekket bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik. Sikkerhetsbrudd og bruk av informasjonssystem i strid med fastlagte rutiner utløser dermed krav til avviksbehandling. Formålet med avviksbehandlingen er å gjenopprette normal tilstand, samt fjerne årsaken til avviket og hindre gjentagelse. Avviksbehandlingen skal dokumenteres, og dokumentasjonen skal brukes som grunnlag for gjennomgang og endring av fastlagte interne rutiner.

Dersom det oppdages avvik som har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal dette rapporteres til Datatilsynet. Uautorisert utlevering vil eksempelvis foreligge når personopplysninger befinner seg utenfor den behandlingsansvarliges kontroll eller at uautoriserte personer har fått tilgang til opplysningene. Dette kan skje ved at personopplysninger feilsendes per e-post, eller ved at riktige forsendelser inneholder personopplysninger om andre. Det kan også skje gjennom ansattes brudd på taushetsplikten.

I tillegg til å implementere sikkerhetstiltak som gjør det mulig å oppdage forsøk på uautorisert bruk av informasjonssystemer, vil avvik kunne oppdages ved interne varslinger. Arbeidsgiver plikter å utarbeide rutiner for intern varsling eller på annen måte legge forholdene til rette for slik varsling om kritikkverdige forhold i virksomheten.[77] Det er dermed påkrevd at NAV har etablert systemer for håndtering av interne varslinger, og for å ivareta de generelle kravene i arbeidsmiljøloven §§ 2-4 og 2-5 om arbeidstakers rett til varsling og vern mot gjengjeldelse. Som nevnt i punkt 5.4 er Internrevisjonen varslingskanal i henhold til NAVs varslingsrutiner.

Som nevnt i punkt 10.2 fastsetter Overordnede Sikkerhetskrav at *"Alle medarbeidere er ansvarlige for å rapportere sikkerhetshendelser og avvik som de oppdager eller blir gjort*

---

[74] *Innebygd personvern* betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. (Https://www.datatilsynet.no/teknologi/innebygd-personvern).

[75] Artikkel 23 i EUs personvernforordning.

[76] Klassifiseringsnivået på informasjonen i det enkelte system avgjør hvorvidt de ikke-funksjonelle kravene er påkrevd eller frivillige

[77] Arbeidsmiljøloven § 3-6.

kjent med til enhetsleder. Sikkerhetshendelser og avvik skal rapporteres så snart som mulig gjennom avviksrapporteringssystemet (ASYS)".

Arbeids- og velferdsetaten har utarbeidet en "*Prosedyre for oppfølging av avvik av etterlevelse*". Hensikten med prosedyren er å beskrive hvordan avvik av etterlevelse av lover og regler, interne styrende dokumenter og operative retningslinjer skal følges opp i etaten. Alle avvik som innebærer brudd på interne krav til beskyttelse av personopplysninger eller informasjonssikkerheten skal følges opp. Det er imidlertid uklart hvor systematisk avvikene i ASYS blir fulgt opp, og hvordan det følges opp at tiltakene fungerer etter hensikten.

De fleste ansatte BDO og Wiersholm har intervjuet er kjent med ASYS, og at avvik kan meldes inn i dette systemet. Flere påpeker at det eksisterer store mørketall hva gjelder avviksrapportering. Samtidig understrekes det at ASYS sitt formål ikke er å ha fullstendig oversikt over avvik, men heller fremheve nødvendige tiltaksområder. Spørreundersøkelsen avdekket at ca. 46 % ikke kjenner til hvordan avvik knyttet til håndtering av personopplysninger skal registreres. I tillegg er det ca. 14 % som ikke vet. Ca. 46 % svarte at de ville ha varslet om eventuelle avvik ved håndtering av personopplysninger. På spørsmål om de ansatte er trygg på å varsle om slike avvik uten å få negative reaksjoner, svarer ca. 50 % "nei" eller "vet ikke".

10.9 Opplæring og kjennskap til regelverket

Etter personopplysningsforskriften § 22-8 (2) skal medarbeidere ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt. Tilfredsstillende opplæring av ansatte er helt sentralt for å implementere tilstrekkelig gode rutiner for personvern og informasjonssikkerhet i organisasjonen.

Det er ikke dokumentert noen plan eller oversikt over hvilken opplæring de enkelte ansatte er pålagt å gjennomføre for å få tilstrekkelig kunnskap i samsvar med de interne retningslinjene[78]. I henhold til Tilleggsinstruks for leder er enhetsledere med personalansvar ansvarlige for at ansatte gis nødvendig opplæring i personvern, informasjonssikkerhet og beredskap.

Nyansatte fra og med 1. juni 2015 omfattes av læringsopplegget "Ny i NAV". Ny i NAV inneholder kurs, samlinger, samtalepakker og e-læringsmoduler som blant annet gjelder temaene personvern, etikk og informasjonssikkerhet. Opplæringen skal gi medarbeiderne nødvendig kunnskap om de krav som følger av lov, forskrift og internt regelverk. Medarbeidere som har vært ansatt før 1. juni 2015 må gjennomføre obligatorisk e-læringskurs i personvern og informasjonssikkerhet [79]. Flere har imidlertid uttalt at kurset er frivillig. Det har derfor trolig ikke blitt formidlet tydelig nok i organisasjonen at opplæringen er obligatorisk, og det er heller ikke etablert et system som sikrer at denne opplæringen blir gjennomført.

For øvrig gis det løpende opplæring i form av publikasjoner på Navets forside. På forespørsel holder representanter fra Sikkerhetsseksjonen innlegg og samtaler på fylkes- og lokalkontor om informasjonssikkerhet, såfremt seksjonen har ledig kapasitet.

Flere ansatte har under intervjuer gitt uttrykk for at det er lokale forskjeller i opplæring om personvern og informasjonssikkerhet. Enkelte mener at e-læringskurs ikke gir den ønskede effekt. Andre har fremhevet e-læringskursene som lærerike og at de får tilstrekkelig veiledning ved behov. Veiledning fra enhetsleder og kolleger inngår i de krav som må stilles til opplæring av ansatte. Flere ansatte ved mindre enheter har gitt uttrykk for at det gis tilstrekkelig veiledning.

[78] Overordnede sikkerhetskrav punkt 4.2.2.

[79] Kravet om obligatorisk sikkerhetskurs fremgår eksplisitt av Mål og disponeringsbrev av 2014. I 2015 ble det henvist til sidene om personvern, informasjonssikkerhet og beredskap på Navet, mens i 2016 fremgår det kun en generell henvisning til informasjon på Navet om krav til virksomhetene.

I spørreundersøkelsen ble det stilt spørsmål om hvor godt de ansatte kjenner til NAVs rutiner og retningslinjer for personvern og informasjonssikkerhet. Ca. 88 % svarte at de kjente rutinene og retningslinjene "godt" eller "meget godt". Selvrapportert kjennskap er dermed på et tilfredsstillende nivå. Ca. 72 % synes retningslinjene er "enkle" eller "meget enkle" å forstå. Dette gir uttrykk for at retningslinjene er tilgjengelige. Ca. 76 % har deltatt i organisert opplæring i personvern og informasjonssikkerhet. Dette er et høyt tall, men samtidig er det ca. 24 % som har svart "nei" eller "vet ikke". Ca. 29 % av ansatte på NAV-kontor i kommune eller bydeler har ikke deltatt i organisert opplæring. Dette tyder på at det ikke er godt nok kommunisert i NAV at e-læringskurs i personvern og informasjonssikkerhet er obligatorisk. Ca. 56 % svarte at de ønsker *mer* opplæring om personvern og informasjonssikkerhet. Dette kan tolkes som en positiv holdning til å lære mer, når tallet ses opp mot den høye andelen som har fått opplæring. Behovet for opplæring er høyest blant ansatte med kort ansiennitet. Videre svarte ca. 78 % at temaene personvern og informasjonssikkerhet diskuteres noen ganger i året eller oftere på deres enhet. I det vesentlige blir temaene tatt opp av kolleger eller lokal ledelse. Kun 10 % svarte at temaene vanligvis ble tatt opp av toppledelsen.

Besvarelsene viser at det gjennomføres opplæring og at temaene er på agendaen, men ikke i tilstrekkelig grad. Gjennomgangen gir samlet sett grunnlag for at opplæringen må anses å være noe fragmentert. Dette har også en klar side mot implementering av det interne regelverket i organisasjonen.

DEL 4 ANBEFALINGER

11. OVERORDNET

NAV har over flere år gjennom rapporter fra både Riksrevisjonen, Datatilsynet og NAVs internrevisjon fått informasjon som klart tilsier at deres behandling av personopplysninger samlet sett ikke er tilfredsstillende. Media har gjennom en rekke artikler over flere år omtalt NAVs behandling av personopplysninger. Det har vært en rekke saker i andre deler av norsk forvaltning knyttet til behandling av personopplysninger, herunder oppslag uten tjenstlig behov. Særlig i tilknytning til helsevesenet og politiet har slike saker vært omtalt av media. Både helsevesenet og politiet er underlagt særlovgivning knyttet til deres behandling av personopplysninger gjennom henholdsvis politiregisterloven[80] som trådde i kraft 2014 og helseregisterloven[81] som trådde i kraft 2015.

Flere konkrete tiltak har blitt planlagt og gjennomført som følge av rapporter fra Riksrevisjonen, Datatilsynet og NAVs Internrevisjon. Det er likevel BDOs og Wiersholms overordnede vurdering og konklusjon at NAV ikke har evnet, i tilstrekkelig grad, å forstå betydningen av hvor sentralt behandling av personopplysninger står i NAVs virksomhet og hvilket ansvar og rettslige plikter som følger av dette.

NAV har flere ganger blitt gjort oppmerksom på forhold som burde foranlediget at brukernes personvern og behandling av personopplysninger ble løftet på den strategiske agenda og dermed gitt arbeidet med å ivareta brukernes personvern den nødvendige prioritet. Dette synes ikke å være gjort.

Per i dag er ikke personvern løftet opp som et kjernepunkt i NAVs overordnede strategidokumenter, ei heller en tilstrekkelig tydelig del av NAVs overordnede mål.

På bakgrunn av NAVs egenart er det er et viktig lederansvar å løfte personvern opp på den strategiske agendaen. NAV må gi arbeidet med oppfølging av BDOs og Wiersholms rapport tilstrekkelig prioritet og ressurser. Formålet er å sikre at alle ledere og medarbeidere i NAV ser på ivaretakelse av brukernes personvern som en naturlig og integrert del av sitt arbeid.

BDOs og Wiersholms viktigste anbefalinger som blant annet følger av manglende strategisk fokus på personvern og behandling av personopplysninger i NAV, er oppsummert i kapittel 12-13 nedenfor[82]. Alle foreslåtte tiltak har en økonomisk side. De vil på linje med alle andre tiltak i NAV være gjenstand for prioriteringer. Det er imidlertid BDOs og Wiersholms klare oppfatning at en rekke av de forhold som påpekes vil kunne avhjelpes/utbedres ved hjelp av forholdsmessige og moderate ressurser sett i forhold til viktighet.

12. ENDRING I ORGANISERINGEN AV PERSONVERNARBEIDET

Gjennomgangen har avdekket organisatoriske utfordringer knyttet til arbeidet med personvern. Dette bygger i stor grad på sammenblandingen av kontrollerende og utøvende funksjoner. Ved vurdering av organisatorisk plassering anbefales det å ta følgende faktorer i betraktning: nærhet til riktig beslutningsnivå, sterk støtte fra virksomhetsledelsen, uavhengighet fra utøvende sikkerhetsarbeid, mulighet for å påvirke beslutninger, mulighet til å få et helhetsbilde samt potensielle interessekonflikter.[83]

Sikkerhetsseksjonen er i dag organisert som en rapporterende enhet under IKT-seksjonen. Leder av Sikkerhetsseksjonen rapporterer direkte til IKT-direktøren. I praksis

[80] Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven).

[81] Lov om helseregistre og behandling av helseopplysninger (helseregisterloven).

[82] BDO og Wiersholm har vurdert om varsel til bruker ved oppslag i Fagsystemene og en eventuell ytterligere lovregulering av NAV-ansattes tilganger og tjenstlig behov kan avhjelpe utfordringene NAV står ovenfor. Forslagene er imidlertid vurdert som lite hensiktsmessige.

[83] Nasjonal Sikkerhetsmyndighet, Veileder i sikkerhetsstyring (2015).

betyr dette at Sikkerhetsseksjonen, som er ansvarlig for at styringssystemet følges, organisatorisk er plassert under NAVs IKT-direktør, som skal følge det samme styringssystemet. Dette er ikke tilfredsstillende. Sikkerhetsseksjonen bør løftes til et høyere nivå som har et styrende/kontrollerende ansvar. Det utøvende ansvaret bør være et linjeansvar i organisasjonen. Videre vurderes ikke Sikkerhetsseksjonens nåværende ressurser og organisering som robust nok til å ha ansvaret for personvern i NAV.

BDO og Wiersholm anbefaler at Sikkerhetsseksjonen omorganiseres til en avdeling som blant annet skal ha det overordnete ansvaret for NAVs arbeid med personvern og informasjonssikkerhet.[84] Det er viktig at en slik avdeling har den nødvendige uavhengighet og det foreslås derfor at avdelingen plasseres på stabsnivå i organisasjonen, og at avdelingsdirektøren har en direkte rapporteringslinje til arbeids- og velferdsdirektøren.

I denne avdelingen bør det opprettes en egen seksjon som har ansvar for personvern. Personvernseksjonen vil ha det overordnete ansvar i NAV for å utarbeide de styrende dokumentene i styringssystemet (strategi og policy) og for å kontrollere de operasjonelle retningslinjene knyttet til personvern i NAV. Seksjonen må tildeles nødvendige ressurser og stillingshjemler for å ivareta sitt ansvar[85].

Det må utvikles en stillingsbeskrivelse for Sikkerhetskoordinatorene som klart definerer ansvarsområde og et eventuelt tilleggsansvar mot den nye seksjonen. BDO og Wiersholm anbefaler også at det utvikles kompetansekrav for medarbeiderne som skal inneha rollen som Sikkerhetskoordinator, og at det tas en vurdering på hvilken stillingsprosent som er nødvendig for å ivareta arbeidet på en tilfredsstillende måte i det aktuelle fylket eller i den aktuelle enhet.

BDO og Wiersholm anbefaler at NAV etablerer et sentralt personvernombud som minimum er en heltidsstilling med ansvar for å påse at NAV etterlever personvernregelverkets krav. Ombudet skal, i tråd med krav og anbefalinger fra Datatilsynet, i tillegg til å være kontaktpunkt for de registrerte ivareta følgende oppgaver[86]:

- Informere og gi råd til virksomheten og de ansatte i saker som handler om personvern
- Bidra til etterlevelse av forordningen og virksomhetens personvernpolitikk
- Gi råd om, og delta i vurderinger av personvernkonsekvenser
- Fungere som kontaktpunkt mellom Datatilsynet og virksomheten

NAV bør også vurdere om det i tillegg til et "sentralt" personvernombud bør opprettes flere personvernombud i organisasjonen (enten basert på "linje", geografi eller basert på andre kriterier), som har direkte rapporteringslinje til det sentrale personvernombudet. De lokale personvernombudenes roller og arbeidsoppgaver må være klart definert i en stillingsbeskrivelse, og det må avsettes tilstrekkelig med ressurser for å ivareta disse oppgavene.

13. FORBEDRING AV STYRINGSSYSTEMET

Det er BDOs og Wiersholms vurdering at etterlevelse av det eksisterende rettslige rammeverk gir tilstrekkelig grunnlag for en forsvarlig behandling av personopplysninger i

[84] Det er BDOs og Wiersholms vurdering at organisering av andre områder enn personvern og informasjonssikkerhet faller utenfor oppdragets mandat. Det anbefales likevel at avdelingen, gjennom opprettelse av separate seksjoner, også får tildelt et helhetlig ansvar for sikkerhet og beredskap. BDO og Wiersholm anbefaler NAV å vurdere om de typer økonomisk kriminalitet som ikke omfattes av NAV Kontrolls ansvarsområde er tilstrekkelig ivaretatt, og om et slikt ansvar også bør tillegges denne avdelingen.

[85] NAV, som offentlig etat, vil bli pålagt å etablere en ordning med personvernombud når EUs personvernforordning trer i kraft i 2018, jf. EUs personvernforordning artikkel 27. Sikkerhetsseksjonen har opplyst at seksjonen skal styrke bemanningen med én ansatt for å håndtere tilpasningene etter EUs nye personvernforordning. Etaten skal også etablere et personvernombud innen forordningen trer i kraft

[86] Etter Datatilsynets definisjon (https://www.datatilsynet.no/Personvernombud/).

NAV. Det anbefales likevel at NAV implementerer en prosess for kontinuerlig forbedring av styringssystemet. Dette inkluderer å etablere konkrete mål som viser i hvilken grad styringssystemet fungerer etter hensikten, samt forbedre sin risikostyringsprosess som en del av styringssystemet. NAV bør også etablere målbare vurderingsparameter forankret hos ledelsen. I dette ligger også at lokale ledere bør måles på sitt arbeid med styringssystemet, for å sikre at dette prioriteres i det daglige arbeidet, samt at det tydeliggjøres hvordan det utøvende sikkerhetsansvaret skal prioriteres i linjen.

Risikovurderinger på informasjonssikkerhet og personvern bør i større grad prioriteres. Dette inkluderer gjennomføring av risikovurderinger for alle viktige systemer, samt et større fokus på dette hos de lokale kontorene.

Etaten har utarbeidet et omfattende internt regelsett som er til dels overlappende. BDO og Wiersholm anbefaler at NAV forenkler strukturen på de operative retningslinjene, herunder reduserer antallet og omfanget av gjeldende retningslinjer. Et hensiktsmessig tiltak er å samle operative retningslinjer, herunder for personvern og informasjonssikkerhet, i en rutinehåndbok som er lett tilgjengelig på Navet. Tilsvarende bør det utarbeides en HMS-håndbok som inneholder informasjon om retningslinjene, rettigheter og plikter knyttet til HMS, i tillegg til beredskap. Med bistand fra HR-avdelingen bør det også utarbeides en mer helhetlig og oppdatert personalhåndbok som gir oversikt over organisasjonsstruktur og de rutiner og retningslinjer som gjelder for de enkelte funksjoner og medarbeiderne generelt.

Opprydningen i det interne regelverket innebærer at samtlige operative retningslinjer bør gjennomgås og enkelte nye rutiner utarbeides. Avvikene fra personopplysningsforskriften som er identifisert i punkt 10.6 bør tas i betraktning slik at retningslinjene tilfredsstiller forskriftens krav.

Videre bør retningslinjene inneholde klart definerte regler. Det er helt sentralt at grunnleggende normer som kravet om tjenstlig behov har et enhetlig innhold. Tilsvarende bør reaksjonsregimet ved brudd på internt regelverk klart og tydelig fremgå av rutinehåndboken. Krav til personvern og informasjonssikkerhet i NAV må være formulert slik at det er enkelt å forstå reglenes innhold og anvende dem i praksis. Eksisterende retningslinjer og rutiner som er overlappende kan med fordel sammenslås og bearbeides for å sikre et enhetlig regelverk.

I forlengelsen av arbeidet med å skape uniforme og oversiktlige regler anbefaler BDO og Wiersholm at NAV forenkler Navets struktur og forbedrer søkefunksjonen. Formålet er å sikre at NAVs interne regelverk reelt sett er tilgjengelig for ansatte til enhver tid.

NAV bør sørge for en mer fullstendig implementering av innebygd personvern i organisasjonen. Det er BDOs og Wiersholms oppfatning at etablering av et mer helhetlig system for tilgangsstyring ligger innenfor det som er mulig under de tekniske og økonomiske forutsetninger NAV opererer under. Eksempelvis bør ansattsperrer benyttes i større grad enn det som er tilfelle i dag for å begrense uautoriserte oppslag på seg selv, familie eller kollegaer på samme enhet.

Videre bør NAV gi klare føringer for prioriteringer av personvern i systemutvikling, eksempelvis bør personvern være viktig parameter i relasjon til fremtidige utskiftninger av NAVs systemer. Per i dag inngår personvern som en del av flere elementer knyttet til informasjonssikkerhet i de "frivillige", ikke-funksjonelle kravene som skal vurderes ved systemutvikling. Det er vår vurdering at personvern-relaterte krav tydeligere må fremgå av de ikke-funksjonelle krav og det må sikres at disse krav ikke feilaktig blir nedprioritert. Det vises her også til vår overordnede vurdering av NAVs manglende strategiske fokus og prioritering av personvern.

14. SYSTEMATISKE LOGGANALYSER

BDO og Wiersholm har gjennomført analyser og identifisert loggoppslag som kan være resultat av uautoriserte oppslag. Mottatt loggdata har blitt koblet sammen med nødvendig tilleggsinformasjon for å kunne gjennomføre analysene. Eksempler på dette er loggdata koblet sammen med oversikt over medarbeidernes relasjoner for å kunne analysere omfang av oppslag på nærstående. Det mottatte datagrunnlaget har tilstrekkelig kvalitet til at NAV skal kunne gjennomføre tilsvarende analyser uten omfattende bearbeidelse, herunder normalisering og datarensking[87].

Analysene som er beskrevet i denne rapporten vil med tilpasninger til lokal infrastruktur dermed kunne implementeres som kontrollfunksjoner i NAVs eksisterende systemer. Dette kan gjøres enten som periodiske eller kontinuerlige kontroller.

Gjennomføring av tilsvarende logganalyser som beskrevet i punkt 2.4.6 antas å kunne ha en betydelig forebyggende effekt mot uautoriserte oppslag. Det vil også være et nyttig virkemiddel for å vurdere hvor effektive implementerte tiltak og opplæringer er, da disse analysene kan gjøres tilbake i tid, samt på ny generert logginformasjon. Slike logganalyser vil i tillegg kunne identifisere mulige tilfeller av uautoriserte oppslag som kan utredes og følges opp videre ved behov. En slik bruk av loggene vil trolig også kunne ha en svært preventiv effekt.

15. IMPLEMENTERING OG OPPLÆRING

Som det fremgår av punkt 10.9, gir Spørreundersøkelsen holdepunkter for at NAV må forbedre opplæring og implementering av retningslinjer for personvern og informasjonssikkerhet. BDO og Wiersholm legger til grunn at dersom tiltak nevnt i punkt 11 gjennomføres, vil behovet for opplæring avta noe. Samtidig er det klart at retningslinjene ikke er godt nok implementert i organisasjonen og at opplæringen er noe fragmentert. Det anbefales derfor at det settes i verk konkrete tiltak på samtlige enheter i NAV for å øke bevisstheten til ansatte om hvilke krav som stilles til personvern og informasjonssikkerhet. Det er naturlig at enhetsledere tildeles ansvaret for dette holdningsskapende arbeidet.

Det anbefales også at det utarbeides mer formelle krav til opplæring og oppdateringskurs for alle knyttet til personvern og informasjonssikkerhet. Dette for å sikre at kompetansen omkring interne krav, personvern og informasjonssikkerhet opprettholdes. I tillegg vil et slikt tiltak samsvare med de ansattes ønske om mer opplæring.

BDO og Wiersholm anser frivillige e-læringskurs som et hensiktsmessig virkemiddel, men dette er ikke alene tilstrekkelig til å oppfylle kravene i personopplysningsloven §§ 13 og 14. Det bør gis opplæring i de sentrale reglene knyttet til tjenstlig behov, herunder i de viktigste rettsreglene. Det er viktig at ansatte ser reglene i sammenheng og at de evner å identifisere problemstillingene i sin arbeidshverdag. Derfor bør opplæringen etter BDOs og Wiersholms oppfatning være praktisk rettet. Videre bør det samtidig gis informasjon om logging av aktivitet i Fagsystemene og reaksjoner på sikkerhetsbrudd. De som er ansvarlige for å vurdere disiplinære reaksjoner bør motta opplæring i relevante retningslinjer.

Opplæringen bør omfatte håndtering av avvik, herunder innføring i avvikssystemet ASYS, jf. punkt 10.7. Opplæringen bør gi en innføring i hvilke avvik som skal rapporteres, slik at avvikssystemet inneholder så representative data som mulig. Det anbefales at resultater og læringspunkter etter håndtering av avvik registreres og systematiseres, i tillegg til å danne erfaringsgrunnlag for opplæringen. Resultatene fra Spørreundersøkelsen tyder på at det må gis mer informasjon om de regler som gjelder

[87] Normalisering (av databaser) er en teknikk for å designe tabeller i databaser slik at man minimerer duplisering av informasjon. Datarensking er en prosess for å sikre at datagrunnlaget ikke inneholder ugyldig informasjon eller feil som kan påvirke analysene.

for varsling. Det må arbeides målrettet med det holdningsskapende arbeidet og ytringsklimaet for å legge til rette for trygg varsling i virksomheten, jf. arbeidsmiljøloven § 3-6.

Videre anbefales det at opplæringen som nevnt ovenfor gjøres obligatorisk for alle ansatte i NAV, uavhengig av stilling og ansettselstid. Når dette er gjennomført på tvers av organisasjonen, kan det være et hensiktsmessig alternativ å inkludere kurset i Ny i NAV. For å unngå at Ny i NAV blir for omfangsrikt, er det sentralt at det ikke er overlapp mellom eksisterende kurs og opplæringen som foreslås her.

Ovenstående tiltak vil føre til at det i større grad arbeides kontinuerlig med de ansattes forståelse av hva som ligger i ansvaret for informasjonssikkerhet og personvern, og hvordan dette skal ivaretas i det daglige arbeidet. Spørreundersøkelsen avdekket at ca. 90 % av de ansatte mente holdningsskapende arbeid vil være et effektivt virkemiddel for å forhindre oppslag uten tjenstlig behov. "Tydeligere ledere" og "opplæring" ble ansett som de mest effektive virkemidler mot oppslag uten tjenstlig behov. Opplæringen bør derfor følges opp med jevnlige diskusjoner og bevisstgjøring på enhetsnivå i regi av enhetsledere. Det holdningsskapende arbeidet bør også ha til formål å skape et trygt ytringsklima hvor ansatte tør å melde fra om avvik uten å risikere gjengjeldelser i strid med arbeidsmiljøloven § 2-5. Det er i tillegg viktig at "tonen fra toppen" er tydelig på at personvern og informasjonssikkerhet skal settes på dagsorden og at brudd på NAVs interne regelverk kan medføre disiplinære reaksjoner. Toppledelsen må også være aktiv i arbeidet med å tilrettelegge for varsling, jf. arbeidsmiljøloven § 3-6.

16. ENHETLIG REAKSJONSMØNSTER

På bakgrunn av det som fremgår av kapittel 8 anbefaler BDO og Wiersholm at NAV utformer et enkelt enhetlig reaksjonsmønster for oppslag uten tjenstlig behov.

Gjennomgangen har avdekket at NAVs kontroll med logger er og har vært utilstrekkelig. Videre er det komplisert, og kanskje heller ikke ønskelig, å begrense den vide informasjonstilgangen som de fleste ansatte i NAV har, og sannsynligvis også kommer til å ha i fremtiden. Nettopp derfor er det viktig at etaten møter eventuelle brudd på forbudet mot oppslag uten tjenstlige behov med mer enhetlige reaksjoner. Den utstrakte delegeringen av ansvaret for å ilegge reaksjoner til lokale enhetsledere – som i stor grad er nødvendig i en organisasjon av NAVs størrelse og struktur – kan medføre ansvarspulverisering. For å motvirke dette, og for å sikre likebehandling på alle nivå i organisasjonen, er det viktig å ha et reaksjonsregime som er så enhetlig som mulig.

HR-avdelingen er tillagt linjeansvar for å ivareta etatens overordnede arbeidsgiverrolle, herunder å yte bistand i prinsipielle saker og å ivareta partsrolle i arbeidsrettssaker[88]. Avdelingen er også tillagt linjeansvar for å utvikle og forvalte etatens metoder og verktøy for forbedringsarbeid, innføring og omstilling[89]. HR-avdelingen er videre tillagt regimeansvar for å tydeliggjøre handlingsregler, rutiner og arbeidsprosesser som skal være felles for etaten arbeidsgiverområdet[90]. Denne avdelingen anses derfor å være best egnet til å utforme et reaksjonsmønster som nevnt. HR-avdelingen bør også gjøre reaksjonsmønsteret kjent blant de enkelte enheter og for samtlige ansatte. Ansvaret for at reaksjonsmønsteret blir implementert og fulgt i praksis tilligger imidlertid den enkelte linje og de enhetsledere som opptrer som arbeidsgiver i det daglige, siden HR-avdelingen ikke har noen styringsfunksjon som sådan.

Selve reaksjonsmønsteret bør utformes så enkelt som mulig. Hvilken reaksjon som skal benyttes i det enkelte tilfelle vil avhenge av sakens alvorlighetsgrad, samt en

[88] Jf. pkt. 4.8 i Ansvarsdokumentet for direktoratet, versjon 1.5.

[89] Jf. pkt. 4.8 i Ansvarsdokumentet for direktoratet, versjon 1.5.

[90] Jf. pkt. 4.8 i Ansvarsdokumentet for direktoratet, versjon 1.5.

interesseavveining mellom virksomhetens behov og den ansattes individuelle forhold. Formålet med reaksjonsmønsteret er imidlertid å tilstrebe at det reageres likt mot like tilfeller av oppslag uten tjenstlig behov i NAV. Skriftlig tjenstlig tilrettevisning bør angis som ufravikelig minimumsreaksjon på samtlige oppslag uten tjenstlig behov. Oppslag som enkelte enhetsledere tidligere kan "ha lukket øynene for"; som oppslag foretatt i opplæringsøyemed eller på de ansatte selv, må omfattes. En ansatt som foretar oppslag uten tjenstlig behov vil altså uavhengig av i hvilken sammenheng, og på hvilke personer oppslaget er blitt foretatt, bli møtt med en arbeidsrettslig reaksjon. Det bør presiseres at alle slike tilrettevisninger skal lagres i den ansattes personalmappe i tråd med regelverket.

Hvorvidt en reaksjon som vurderes gitt kun vil representere en skriftlig tilrettevisning eller en ordenstraff når den gis til statlige ansatte, må vurderes i hvert enkelt tilfelle. Det avgjørende i den forbindelse er bl.a. hvorvidt reaksjonen tenkes utformet slik at den først og fremst skal ha som siktemål å klargjøre nærmere innholdet og omfanget av tjenestemannens tjenesteplikter, eller om sanksjonspreget vil være sterkest. I sistnevnte tilfelle vil reaksjonen være en ordensstraff, og reglene for slike etter tjenestemannsloven og forvaltningsloven må da overholdes. Den samme vurderingen må gjennomføres dersom det i ettertid oppstår spørsmål om en reaksjon gitt som skriftlig tilrettevisning i realiteten representerte en ordensstraff, som dermed skulle vært behandlet etter reglene i tjenestemannsloven og forvaltningsloven.

Reaksjonsmønsteret bør videre gi anvisning på at oppsigelse, avskjed og politianmeldelse skal vurderes ved alvorlige tilfeller av oppslag uten tjenstlig behov og/eller gjentatte tilfeller av dette.

Basert på undersøkelsene, er inntrykket at de fleste NAV-ansatte allerede er godt kjent med forbudet mot å gjøre oppslag uten tjenstlig behov, selv om det kan være noe usikkerhet knyttet til grensetilfeller som oppslag på en selv eller oppslag gjort i opplæringsøyemed. Følgelig kan alle enhetsledere og andre som utøver arbeidsgiveransvaret i NAV allerede i dag reagere på eventuelle brudd.

I tillegg vil alle som utøver arbeidsgiveransvar i NAV få et klart signal om at det *skal* og *må* reageres på samtlige slike brudd. HR-avdelingen har som tidligere nevnt ingen samlet oversikt over hvor mange ansatte som hvert år mottar arbeidsrettslige reaksjoner som en følge av oppslag uten tjenstlig behov. Generelt bør NAV utvise tilbakeholdenhet med å pålegge ledere i etaten for omfattende rapporteringskrav. Med et reaksjonsmønster som foreskrevet, vil imidlertid enhetsledere sannsynligvis i større grad enn tidligere ilegge ansatte arbeidsrettslige reaksjoner som en følge av oppslag uten tjenstlig behov, særlig skriftlige tilrettevisninger. BDO og Wiersholm anbefaler derfor at samtlige enhetsledere innrapporterer saker hvor ansatte er blitt vurdert oppsagt eller avskjediget som en følge av oppslag uten tjenstlige behov til Arbeidsgiverseksjonen.