

Endelig tilsynsrapport		
Saksnummer: 23/00708 Dato for kontroll: 06.09.2023 Rapportdato: 27.11.2023	Kontrollobjekt: Arbeids- og velferdsdirektoratet Sted: Fyrstikkalléen 1, 0661 Oslo	Utarbeidet av: Ingrid H. Espolin Johnson Kristin Karlsen Lindberg Siri Aasness Narjes Al-Sultan Camilla Nervik

Innhold

1	Innledning	3
2	Bakgrunn – Om betydningen av konfidensialitetssikring i NAV	3
3	Deltakere	4
4	Internkontroll og ansvarsforhold.....	4
4.1	Rettslig grunnlag	4
4.2	NAVs styringssystem.....	5
4.2.1	Faktiske forhold	5
4.2.2	Datatilsynets vurdering	6
4.3	Ansvarsforhold.....	7
4.3.1	Faktiske forhold	7
4.3.2	Datatilsynets vurdering	8
4.4	Ledelsens gjennomgang	8
4.4.1	Faktiske forhold	8
4.4.2	Datatilsynets vurdering	8
4.5	Oppsummering og konklusjon	9
5	Tilgangsstyring	9
5.1	Rettslig grunnlag	9
5.2	Overordnede føringer for tilgangsstyring i NAV	11
5.2.1	Faktiske forhold	11
5.2.2	Datatilsynets vurdering	12
5.3	Tildeling og opplæring	13
5.3.1	Faktiske forhold	13
5.3.2	Datatilsynets vurdering	16
5.4	Prinsippet «tjenstlig behov» og landsdekkende tilganger	17
5.4.1	Faktiske forhold	17

5.4.2	Datatilsynets vurdering	18
5.5	Beskyttelse av personer med fortrolig og strengt fortrolig adresse.....	19
5.5.1	Faktiske forhold	19
5.5.2	Datatilsynets vurdering	20
5.6	Beskyttelse av egne ansatte	20
5.6.1	Faktiske forhold	20
5.6.2	Datatilsynets vurdering	21
5.7	Andre grupper med særskilt behov for konfidensialitetsvern	21
5.7.1	Faktiske forhold	21
5.7.2	Datatilsynets vurdering	22
5.8	Revisjon.....	22
5.8.1	Faktiske forhold	22
5.8.2	Datatilsynets vurdering	23
5.9	Oppsummering og konklusjon	24
6	Logg	25
6.1	Rettslig grunnlag	25
6.2	Faktiske forhold.....	25
6.3	Datatilsynets vurdering	26
6.4	Oppsummering og konklusjon	26
7	Loggkontroll	26
7.1	Rettslig grunnlag	26
7.2	Faktiske forhold.....	26
7.3	Datatilsynets vurdering	27
7.4	Oppsummering og konklusjon	28

1 Innledning

Datatilsynet gjennomførte et stedlig tilsyn hos Arbeids- og velferdsetaten (NAV) 6. september 2023, i kraft av myndighet gitt i personvernforordningen artikkel 57 og 58, jf. personopplysningsloven § 20. Formålet med tilsynet var å kontrollere om NAV sikrer tilfredsstillende konfidensialitet i IT-løsningene («fagsystemene») som benyttes til å behandle personopplysninger i forbindelse med tjenesteyting. Vi undersøkte NAVs tekniske og organisatoriske tiltak knyttet til tilgangsstyring, logg og loggkontroll, jf. personvernforordningen artikkel 32 og artikkel 5 nr. 1 bokstav f. Vi undersøkte særskilt NAVs evne til å tilpasse sikkerhetsnivået for personer som har et ekstra konfidensialitetsbehov (f.eks. personer som lever på fortrolig og strengt fortrolig adresse, egne ansatte og offentlig kjente personer).

Vi undersøkte videre om NAV har etablert et egnet styringssystem for disse formålene, jf. personvernforordningen artikkel 24 og artikkel 5 nr. 2.

Tilsynet var avgrenset til behandling av personopplysninger i fagsystemer som inngår i den statlige delen av NAVs tjenesteyting.

NAV hadde på forhånd fremlagt dokumentasjon i henhold til pålegg fra Datatilsynet i brev 1. mars 2023, herunder detaljerte opplysninger om 55 statlige fagsystemer. Gjennom de detaljerte opplysningene fikk vi blant annet informasjon om formålet med behandling av personopplysninger i de enkelte systemene, antall registrerte i hvert system og antall ansatte med tilgang. Denne informasjonen bidro til å synliggjøre hvorvidt NAV i praksis følger sine egne retningslinjer og rutiner for konfidensialitetssikring. Informasjonen indikerte samtidig hvor personvernrisikoen er størst, slik at vi kunne rette kontrollen mot disse områdene.

Den forhåndsinnsendte dokumentasjonen, informasjonen som fremkom under samtalene med NAV 6. september 2023 og ettersendte dokumenter utgjør grunnlaget for denne tilsynsrapporten.

2 Bakgrunn – Om betydningen av konfidensialitetssikring i NAV

NAV forvalter store mengder opplysninger om hele Norges befolkning. En stor andel av disse personopplysningene er svært sensitive for den det gjelder. NAVs behandlingsansvar innebærer plikter til å ivareta disse opplysningene på en sikker måte i tråd med personvernregelverket. Befolkningen skal kunne ha tillitt til at offentlige myndigheter opptrer profesjonelt og kun bruker personopplysningene våre til lovlige formål.

Samtidig kan balansen mellom effektivitetshensyn og konfidensialitetshensyn utfordre personvernet. NAV har mer enn 20 000 ansatte og rundt 200 ulike datasystemer for hele sin virksomhet. NAV har en kompleks organisasjonsform gjennom underliggende enheter, samspillet med kommunen og mange andre aktører. Dette medfører at det må stilles strenge krav til tilgangsstyring, logging og loggkontroll hos NAV.

Datatilsynet mottar mange henvendelser, herunder klager fra registrerte og varsler fra ansatte i NAV, som på ulike måter problematiserer konfidensialitetssikringen i NAVs fagsystemer. Datatilsynet gjennomførte et stedlig tilsyn hos NAV i 2011 hvor dette var tema.¹ I etterkant av dette har Datatilsynet behandlet en rekke enkeltsaker, men ikke gjennomført noen helhetlig kontroll. På denne bakgrunnen fant vi det riktig og hensiktsmessig å gjennomføre et nytt stedlig tilsyn hos NAV.

3 Deltakere

Fra Datatilsynet deltok:

- Ingrid H. Espolin Johnson, juridisk rådgiver
- Kristin Karlsen Lindberg, juridisk seniorrådgiver
- Siri Aasness, juridisk seniorrådgiver
- Narjes Al-Sultan, rådgiver
- Camilla Nervik, seksjonssjef

Fra NAV deltok:

- Odd-Erik Røste, prosjektleder
- Marianne Fålun, økonomi- og styringsdirektør
- Espen Bago, fagdirektør
- Petter Hafskjold, avdelingsdirektør
- Jon Hofstad, sikkerhetssjef
- Ida Stenerud, løsningsarkitekt
- Anders Holt, personvernombud
- Mari Kristiansen, juridisk rådgiver
- Benjamin Jensen Scheich, juridisk rådgiver
- Eivind Staff, sikkerhetsarkitekt
- Mariell D. Østhagen, rådgiver

Økonomi- og styringsdirektøren deltok kun i åpningsmøtet. Ellers var ingen fra NAVs sentrale ledelse tilstede under tilsynet.

4 Internkontroll og ansvarsforhold

4.1 Rettslig grunnlag

Den behandlingsansvarlige har etter personvernforordningen ansvar for å sikre at de grunnleggende prinsippene for behandling av personopplysninger overholdes og skal kunne «påvise» at dette gjøres, jf. artikkel 5 nr. 2.

Ansvarer innebærer en forpliktelse til å gjennomføre «egne tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med» forordningen, jf. artikkel 24 nr. 1. Det skal i den forbindelse tas hensyn til behandlingens art, omfang, formål og

¹ Saksnummer 11/00797.

sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

Personvernforordningen pålegger den behandlingsansvarlige å iverksette «egne retningslinjer» dersom det «står i et rimelig forhold til behandlingsaktivitetene», jf. artikkel 24 nr. 2. Tilsvarende kan leses ut av artikkel 32 nr. 4, som sier at den ansvarlige må treffe tiltak for å sikre at de som handler for dem kun behandler personopplysninger etter instruks.

Det stilles også krav om at tiltakene gjennomgås og oppdateres ved behov, jf. artikkel 24 nr. 1 siste setning og artikkel 32 nr. 1 bokstav d.

Delegering av ansvar og fordeling av oppgaver og roller innenfor etterlevelse av personvernregelverket forutsettes å være klarlagt og dokumentert.

Tekniske og organisatoriske tiltak etter artikkel 24 omtales ofte som internkontroll, styringssystem, kvalitetssystem eller rammeverk (heretter «styringssystem»). Systematikken skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse av personvernregelverket. Tiltakene skal også være de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Et velfungerende styringssystem består av såkalte styrende, gjennomførende og kontrollerende rutiner, retningslinjer eller prosedyrer (heretter «rutiner»).

4.2 NAVs styringssystem

4.2.1 Faktiske forhold

NAV opplyser at de har et styringssystem som de selv har utviklet. Under tilsynet ble det henvist til figuren «Styringsmodell for sikkerhet» fra dokumentet *Styringsdokument for sikkerhet i NAV* for illustrasjon.

Styringssystemets dokumenter er innordnet i et tretrinns hierarki. Toppnivået (nivå 1) består av strategiske sikkerhetsmål, prinsipper og organisering. Nivå 2 består av overordnede krav innenfor forskjellige områder, inkludert standarddokumenter, retningslinjer, rutiner og prosedyrer. Nivå 3 består av verifikasjonsdokumenter i form av oversikter og rapporter. Dokumentene finnes på NAVs intranett, «Navet».

På toppnivået finnes to sentrale dokumenter for etterlevelse av personvernregelverket:

- *Styringsdokument for personvern i Arbeids- og velferdsetaten* (godkjent 17.03.2023)
- *Styringsdokument for sikkerhet i NAV* (godkjent 19.11.2020)

Dokumentene må ses i sammenheng.

Styringsdokumentet for personvern beskriver rammer, mål, myndighet og ansvar som ligger til grunn for arbeidet i etaten². Dokumentet skal bidra til å fastsette mål for personvern og aktiviteter for å nå disse målene. Videre beskriver dokumentet roller og ansvar, herunder hvem som har det utøvende ansvaret for etterlevelse av personvernlovgivningen.

Dokumentet gir en beskrivelse av styringssystemet og inneholder beskrivelser av ledelsens gjennomgang av området. Det går frem at dokumentasjonen skal være lett tilgjengelig for alle ansatte i NAV.

I den ettersendte dokumentasjonen fremgår det at NAV anser at de har etablert to styringssystemer for henholdsvis personvern og informasjonssikkerhet. Dette ble ikke adressert under det stedlige tilsynet, og Datatilsynet vil derfor ikke gå nærmere inn på temaet i kontrollrapporten.

NAV medgir at gjeldende rutiner verken er systematiske eller dekkende, men at styringssystemet har elementer som anses tilstrekkelige. NAV opplyser samtidig at de ikke har noe verktøy som gjør det enkelt å holde oversikt.

På spørsmål under tilsynet svarte NAV at de ikke anser dagens styringssystem som tilfredsstillende. De svarte også at styringssystemet er lite tilgjengelig og lite brukt av ansatte. NAV opplyste at de mangler et helhetlig «kvalitetssystem».

Dette er også påpekt i NOU 2023: 11, *Raskt og riktig*, i mars 2023. Utredningen er laget av et utvalg som ble satt ned av regjeringen for å gjennomgå klage- og ankesystemet i Arbeids- og velferdsetaten og Trygderetten. Utvalget konkluderer med at NAVs arbeid med å øke kvalitet (i ytelsesforvaltningen) fremstår som lite helhetlig og systematisk. Utvalget har anbefalt at det blir utarbeidet et helhetlig kvalitetssystem, som skal sikre fokus på kvalitet i tjenestene til brukerne, samt prosessene bak disse.

PwC gjennomførte også i 2020 en modenhetsvurdering etter bestilling fra NAV. Vurderingen er unntatt offentlighet og har ikke vært relevant for gjennomføringen av tilsynet fra Datatilsynet, men vi vil trekke frem at det også der påpekes et klart behov for et bedre styringssystem.

NAV arbeider med å forbedre sitt styringssystem.

4.2.2 Datatilsynets vurdering

Personvernregelverket legger opp til at det skal gjøres konkrete vurderinger knyttet til hvilke organisatoriske tiltak styringssystemet må inneholde, ettersom tiltakene skal «stå i et rimelig forhold til behandlingsaktivitetene». Det er opp til den behandlingsansvarlige å sikre at systemet er egnet til å oppfylle sin hensikt i virksomheten.

NAV har en kompleks organisasjonsform med mange underliggende enheter spredd geografisk over hele landet. For den statlige delen av NAV, er Arbeids- og

² Betegnelsen «etaten» inkluderer alle statlige organer som er underordnet direktoratet.

velferdsdirektoratet ved øverste leder behandlingsansvarlig etter personvernregelverket. Det praktiske og daglige ansvaret for etterlevelse av regelverket er imidlertid i stor grad delegert.

Et velfungerende og robust styringssystem for tekniske og organisatoriske tiltak er nødvendig for at den behandlingsansvarlige skal kunne sikre og påvise at personvernregelverket er ivaretatt.

NAVs organisering og struktur nødvendiggjør et omfattende styringssystem. I vurderingen av hva styringssystemet må inneholde, skal det tas hensyn til personopplysningene NAV behandler og deres art, omfang og formål. Det skal også tas hensyn til risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter.

Tatt i betraktning at NAV behandler opplysninger om hele Norges befolkning, i alle livsfaser, herunder betydelige mengder opplysninger innenfor det som betegnes som særlige kategorier, stilles det strenge krav til hvilke organisatoriske og tekniske tiltak NAV skal etablere.

Datatilsynet vurderer at det er elementer i styringssystemet som er velfungerende og som er tilfredsstillende organisatoriske tiltak. Det er for eksempel lagt frem rutiner og enkelte styrende dokumenter som er naturlige elementer i et styringssystem. Datatilsynet ser også at systematikken i styringssystemet NAV har presentert kan være egnet for formålet.

Gjennom tilsynet går det imidlertid frem at NAVs styringssystem ikke anses helhetlig, og at det heller ikke dekker alle områder. Videre går det frem at styringssystemet har mangler knyttet til tilgjengelighet og systematikk, og at det eksisterende verktøyet ikke er egnet.

Det fremstår klart for Datatilsynet at NAV gjennom sitt styringssystem ikke i tilstrekkelig grad har etablert egnede tekniske og organisatoriske tiltak for å sikre og påvise at deres behandling av personopplysninger utføres i samsvar med personvernforordningen, jf. personvernforordningen artikkel 24 nr. 1 og 2. Vi har i denne vurderingen sett særlig hen til hvilke personopplysninger NAV har behandlingsansvaret for, omfanget av behandlingen og NAVs komplekse organisasjonsform.

Dette synet understøttes av NOU 2023:11, og av PwCs vurderinger i rapporten *Modenhetsvurdering sikkerhet* fra 2020.

4.3 Ansvarsforhold

4.3.1 Faktiske forhold

Gjennom dokumentasjonen som har vært relevant under tilsynet, fremgår det klart at det er øverste leder i Arbeids- og velferdsdirektoratet som er behandlingsansvarlig for etatens behandling av personopplysninger.

NAV opplyser at de har en styringsmodell som innebærer at linjeledelsen tar ansvar innenfor sin egen linje, inkludert ansvaret for personopplysningssikkerhet.

I styringsdokumentet for personvern konkretiserer NAV hva oppgavene og ansvaret innebærer på personvernområdet og hvordan dette er fordelt. Dokumentet viser til at den enkeltes ansvar og oppgaver er beskrevet i *Ansvarsdokument for direktoratet*. Styringsdokumentet beskriver detaljerte oppgaver og ansvar knyttet til de forskjellige enhetene og nivåene i etaten, fra øverste direktør og til den enkelte medarbeider.

4.3.2 Datatilsynets vurdering

Ansvarsfordelingen for behandling av personopplysninger er beskrevet i *Styringsdokument for personvern i Arbeids- og velferdsetaten*. Datatilsynet vurderer at NAV har et oversiktlig bilde over plassering av behandlingsansvar og hvor i organisasjonen oppgaver og ansvar er delegert.

Det fremstår noe uklart hvordan de ulike delegeringene følges opp med rapportering på etterlevelse. Dette har imidlertid ikke vært et tema under kontrollen.

Datatilsynet avdekket ikke avvik knyttet til plassering av ansvar under tilsynet.

4.4 Ledelsens gjennomgang

4.4.1 Faktiske forhold

NAV opplyste at ledelsens gjennomgang av personvernområdet skjer årlig. Hver direktør redegjør for sitt område. Resultatet fra gjennomgangen følges opp med konkrete tiltak ved behov. NAV opplyser at gjennomgangen er grundig, og at den blant annet inneholder rapportering på status på pågående tiltak og eventuelle nye områder som må forbedres.

Eventuelle tiltak følges opp gjennom tertialrapportering til ledelsen.

NAV har i etterkant av tilsynet sendt en beskrivelse av hvordan ledelsens gjennomgang utføres. Det går frem av beskrivelsen at det «[h]vert år utarbeides en rapport som danner grunnlaget for «Ledelsens gjennomgang» av personvern. «Ledelsens gjennomgang» blir gjennomgått og forankret årlig i d-møtet».

NAV opplyser samme sted at «[h]ensikten med den årlige «Ledelsens gjennomgang» er å følge opp mål og føringer som direktoratets ledelse har satt innen personvern i det årlige mål- og disponeringsbrevet og gjennomgå behov for korrigerende tiltak, slik at risikonivået og de risikoreducerende tiltak som skal iverksettes, er godt forankret. Gjennomgangen skal bidra til at Arbeids- og velferdsetaten har hensiktsmessig, tilstrekkelig og effektiv internkontroll på området.»

Under tilsynet ble det påpekt at også personvernombudet, omtrent hver sjettede uke, rapporterer til direktøren på aktuelle tema. Personvernombudet definerer innholdet i møtet.

4.4.2 Datatilsynets vurdering

NAV har etablert en rutine for ledelsens gjennomgang på personvernområdet. Av den beskrivelsen vi har mottatt i etterkant av tilsynet, går det frem at en del av innholdet i

rapporten som blir lagt frem for ledelsen er basert på tilbakemeldinger og innspill fra avdelingene i direktoratet og andre NAV-enheter.

Det er ikke fremlagt dokumenterte rutiner på hvordan alle underliggende ledd i ansvarskjeden rapporterer oppover til ledelseslinjene de tilhører. Datatilsynet anser at en slik rapportering vil være et nødvendig element, særlig sett hen til den komplekse organisasjonen i NAV, for at den behandlingsansvarlige kan kontrollere eller vurdere og deretter påvise at de etablerte tiltakene i etaten fungerer etter sin hensikt. Dette har ikke vært konkret omhandlet under tilsynet, og vi vil derfor kun presisere at dette er et tiltak NAV må vurdere.

Datatilsynet avdekket ikke avvik knyttet til NAVs rutine for ledelsens gjennomgang under tilsynet.

4.5 Oppsummering og konklusjon

Datatilsynet har under tilsynet funnet at NAV har et etablert styringssystem, og at deler av det er egnede organisatoriske tiltak for å påvise og sikre etterlevelse av enkelte deler av personvernregelverket.

Datatilsynet merker seg at mangler ved NAVs styringssystem også har vært påpekt i modenhetsvurderingen «Modenhetsvurdering sikkerhet» fra PwC i 2020 og i NOU 2023:11.

Datatilsynet har også merket seg at NAV har igangsatt et arbeid med å utbedre manglende i sitt styringssystem. På tross av at dette arbeidet har pågått i lang tid, er manglene ikke avhjulpet.

Datatilsynets konklusjon er at det gjennom tilsynet har kommet frem at det etablerte styringssystemet har svakheter og mangler, både i den overordnede systematikken og i konkrete rutiner, se punkt 5.2.2, 5.3.2, 5.4.2 og 5.8.2.

- **Avvik 1:** NAV har ikke i tilstrekkelig grad etablert et styringssystem som gir egnede tekniske og organisatoriske tiltak for å sikre og påvise at deres behandling av personopplysninger utføres i samsvar med personvernforordningen, jf. artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2.

5 Tilgangsstyring

5.1 Rettslig grunnlag

Det overordnede kravet etter personvernforordningen artikkel 32 nr. 1 er at den behandlingsansvarlige gjennomfører «egne tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen» ved behandlingen av personopplysninger.

Dette gir anvisning på en risikobasert og skjønnsmessig tilnærming. Hensikten er at sikkerhetstiltakene skal stå i et rimelig forhold til den konkrete risikoen ved behandlingen.

Dette forutsetter at den behandlingsansvarlige gjennomfører risikovurderinger, hvilket også er et krav etter artikkel 32 nr. 2.

I artikkel 32 nr. 1 bokstav a til d er det opplistet fire sikkerhetstiltak som alltid bør vurderes. I denne konkrete sammenhengen er bokstav b og d særlig relevante.

Bokstav b stiller krav om at den behandlingsansvarlige har iverksatt tiltak som gir «evne til å sikre vedvarende konfidensialitet (...)» hvor risikovurderingen tilsier at det er nødvendig.

Bokstav d stiller krav om at den behandlingsansvarlige etablerer «en prosess for regelmessig testing, analysering og vurdering av hvor effektive» de øvrige sikkerhetstiltakene er.

Personvernforordningen stiller ikke spesifikke krav til det nærmere innholdet i sikkerhetstiltakene. For offentlige myndigheter gjelder likevel en plikt til å bruke etablerte standarder ved anskaffelse, utvikling, oppsett, drift og bruk av IT-løsninger, jf. forskrift 5. april 2013 nr. 959 om IT-standarder i offentlig forvaltning § 14. Det finnes en rekke slike standarder for personopplysningssikkerhet, som gjennomgående stiller krav om at tiltak som tilgangsstyring, logging og loggkontroll er på plass, se for eksempel ISO/IEC 27002:2022 kapittel 5 og 8. Det er på det rene at tilgangsstyring er et nødvendig element i tiltakene som er påkrevd etter artikkel 32.

Summen av tiltak knyttet til tilgangsstyring, logging og loggkontroll avgjør om konfidensialitetsnivået er tilfredsstillende. Dette innebærer at loggkontrollen til en viss grad kan tilpasses valgt nivå av tilgangsstyring. Vide tilganger tilsier en streng loggkontroll. En streng og snever tilgangsstyring kan tilsi et mindre behov for å kontrollere logger.

Tekniske tiltak må suppleres med organisatoriske tiltak som opplæring og rutiner. Dette krever et egnet styringssystem. Kvaliteten på styringssystemet har derfor innvirkning på hvorvidt sikkerhetstiltakene anses tilfredsstillende.

Det såkalte konfidensialitetsprinsippet følger av personvernforordningen artikkel 5 nr. 1 bokstav f, som lyder:

«Personopplysninger skal ... behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling ... ved bruk av egnede tekniske eller organisatoriske tiltak ...».

Sikkerhetstiltakene må derfor ta høyde for og innrettes mot hva som utgjør en uautorisert eller ulovlig behandling. Prinsippet kalt «tjenstlig behov», som blant annet kommer til uttrykk gjennom regler om taushetsplikt, og nødvendighetskriteriet i dataminimeringsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav c, står sentralt i den sammenhengen.

5.2 Overordnede føringer for tilgangsstyring i NAV

5.2.1 Faktiske forhold

I henhold til pålegg fra Datatilsynet 1. mars 2023 fremla NAV 31. mai 2023 sine styrende retningslinjer for tilgangskontroll, dokumentene *Tilgangskontroll* og *Autorisasjon*. Begge retningslinjene er datert 18. desember 2010 og merket som versjon 1.0.³

Den 27. august 2023 mottok Datatilsynet ytterligere to dokumenter fra NAV: retningslinjen *Standard for tilgangsforvaltning* (versjon 1.0, datert 30. juni 2023) og *Styringsdokument for sikkerhet i NAV* (versjon 1.0, datert 19. november 2020).⁴

Under tilsynet forklarte NAV at styringsdokumentet ligger på nivå 1 i dokumenthierarkiet. Retningslinjene ligger på nivå 2.

NAV bekreftet under tilsynet at retningslinjene ikke har blitt revidert siden 18. desember 2010. Dette ble forklart med at retningslinjene er knyttet til systemet Identrutina (NAVs system for tildeling av tilganger), og at Identrutina heller ikke er endret siden 2010. NAV har et mål om at retningslinjene skal erstattes over tid.

I notatet *Tilgangsstyring og logging i NAV*, som er del av svaret på Datatilsynets pålegg 1. mars 2023, beskriver NAV at tilgangsstyringen er en felles prosess, og at det derfor i liten grad finnes fagsystemspesifikke rutiner for dette. Fellesløsningene forvaltes av egne produktteam.

Produktteamene definerer, utvikler og er ansvarlige for hvilke muligheter for tilgangsstyring som finnes, og på hvilke måter ansatte kan oppnå tilgang til ulike applikasjoner. NAV forklarte at de også skal fange opp innretninger som avviker fra standardløsninger.

Produktteamene er tverrfaglige og består av utviklere og representanter fra aktuelle fagområder. NAV opplyste under tilsynet at disse arbeider etter særskilte retningslinjer. Disse retningslinjene ble ettersendt 14. september 2023. Dokumentet har ingen tittel og er ikke datert. Det inneholder en liste med standard spørsmål ved «*opprettelse av tilgangsstyring via Remedy Brukeradministrasjon*». Remedy Brukeradministrasjon og Identrutina er det samme systemet, men omtales med forskjellig navn avhengig av konteksten det beskrives i.⁵

NAV har etablert roller for tilgangsstyring på flere nivåer, f.eks. geografi, stilling/rolle og opplysningstype. Teknisk sett finnes det derfor en rekke muligheter for å styre tilganger.

I tilsynet påpekte Datatilsynet at risikoen ved NAVs behandling av personopplysninger varierer med de ulike formålene behandlingen tjener, hvor sensitive personopplysningene er, antall registrerte, osv. Det går frem av NAVs retningslinjer i dokumentene *Tilgangskontroll* og *Autorisasjon* at tilganger skal ha en viss forankring i klassifisering av risiko.

³ Endret etter innspill fra NAV 22.11.23.

⁴ Endret etter innspill fra NAV 22.11.23.

⁵ Endret etter innspill fra NAV 22.11.23.

På spørsmål om hva de viktigste mekanismene er for å sikre at sikkerhetstiltakene, i form av tilgangsstyring, tilpasses risikoen i hvert enkelt system, svarte NAV at produktteamene som forvalter de enkelte fagsystemene må vite om de jobber med noe innenfor eller utenfor «normalen». Produktteamene skal konsultere sikkerhetsseksjonen eller IT-seksjonen ved behov.

NAV opplyser at produktteamene har et rammeverk som sier at bestemt type informasjon, for eksempel «fortrolig» og «strengt fortrolig» adresse (kode 6 og 7), skal skjermes. Når produktteamene lager et nytt system, får de spørsmål om systemet skal behandle ekstra sensitiv informasjon. De må også ta stilling til om det skal være noen begrensninger i hvem som skal kunne bestille tilgang.

5.2.2 Datatilsynets vurdering

Som påpekt ovenfor i punkt 4.2.2, vurderer Datatilsynet at NAVs styringssystem er ufullstendig, og har mangler knyttet til tilgjengelighet, systematikk og egnethet. Disse manglene synliggjøres konkret i NAVs styrende dokumenter for tilgangsstyring.

Styrende dokumenter skal definere retningen på arbeidet og danne et tydelig rammeverk for hele virksomheten. Dette er særlig viktig når de tekniske tiltakene krever riktig bruk for å virke etter sin hensikt. Kombinasjonen av tekniske og organisatoriske tiltak skal ha som mål å gi tilstrekkelig konfidensialitetsbeskyttelse i systemene.

Datatilsynet vurderer at det er enkelte uklarheter mellom dokumentene på nivå 1 og 2 vedrørende hvilke premisser som skal ligge til grunn for tilgangsstyring i NAV. Dette gjør rammeverket utydelig og skaper usikkerhet om hvordan tilgangsstyringen skal innrettes.⁶

Gjennomgangen har vist at produktteamene som utvikler fagsystemene ikke har rutiner eller instruksjoner som gjelder utforming av tilgangsstyringen på en måte som hensyntar den varierende risikoen ved behandlingen av personopplysninger. Listen med standard spørsmål ved «*opprettelse av tilgangsstyring via Remedy Brukeradministrasjon*» er knyttet til interne brukere av systemet. Det fremstår som at risikoene for den registrertes rettigheter og friheter er ikke med i disse vurderingene. Den risikobaserte tilnærmingen som styringsdokumentene på nivå 2 legger opp til er dermed ikke videreført i praksis.

Det er konkrete risikovurderinger som skal vise hvilke tiltak som er nødvendige i tilknytning til behandlingen av personopplysninger. Manglende rutiner på dette området anses derfor som et avvik fra sikkerhetskravene i personvernforordningen artikkel 32 nr. 1.

I lys av den iboende høye risikoen ved NAVs behandling av personopplysninger og NAVs komplekse organisasjonsform, anser Datatilsynet at NAVs styrende rammeverk for tilgangsstyring, som organisatorisk tiltak for å supplere de tekniske tiltakene, ikke er egnet for å oppnå tilfredsstillende personopplysningssikkerhet, jf. personvernforordningen artikkel 32 nr. 1.

⁶ Endret etter innspill fra NAV 22.11.23.

Det er også en klar mangel at retningslinjene ikke er revidert siden 2010. Det er alminnelig praksis at sentrale retningslinjer revideres jevnlig og ved behov. NAV erkjenner selv at retningslinjene er utdaterte. Dette utgjør et brudd på kravene til regelmessig revisjon etter personvernforordningen artikkel 32 nr. 1 bokstav d.

5.3 Tildeling og opplæring

5.3.1 Faktiske forhold

I notatet *Tilgangsstyring og logging i NAV* er prosessen for tildeling av tilganger forklart slik på side 2:

«Tilgangsstyring er prosessen med å tildele og vedlikeholde tilganger. I NAV er dette én felles prosess. Identrutina og AD (Active Directory) brukes for henholdsvis tildeling og lagring av tilganger som benyttes på tvers av fagsystemer.

(...)

NAV's primære system for tildeling av tilganger er Identrutina. Identrutina tilbyr en arbeidsflyt der en identadministrator velger hvilke tilganger en medarbeider skal ha. Ett kryss/valg i Identrutina fører typisk til at brukeren meldes inn i én eller flere AD-grupper. (...) Noen AD-grupper «eies» av ett team og brukes kun av ett fagsystem, mens andre tilganger brukes på tvers.»

Dette er utdypet på side 3 og 4:

«Teamet som har ansvar for et fagområde i NAV, har ansvar for å bestemme hvilke fagsystemer som skal støtte fagområdet. Når et fagsystem etableres og videreutvikles, bestemmer teamet hvilke tilgangsnivåer som skal være tilgjengelige for brukerne. Disse tilgangsnivåene er tett knyttet til hvordan fagområdet er organisert i NAV. Et viktig prinsipp som benyttes her er "tjenstlig behov". Dette betyr at innenfor et gitt tilgangsnivå, skal det kun være tilgang til informasjon og funksjonalitet som er nødvendig for å løse arbeidsoppgavene til medarbeideren på det gitte tilgangsnivået.

(...)

Det er teamet som eier et fagsystem, som bestemmer hvilke enheter som skal ha lov til å tildele tilganger til teamets applikasjoner. Enhetenes leder har det formelle ansvaret for å godkjenne alle tildelinger til medarbeidere i enheten. I noen tilfeller delegerer lederen godkjenningen til en identadministrator.»

Rutinen *Ident- og tilgangsadministrasjon* (Identrutina) beskriver blant annet identadministratorenes hovedoppgaver og ansvarsområder, regler for hvor mange identadministratorer det kan være på en enhet, delegeringsmyndighet og hvordan en går fram for å bestille tilganger og gjør endringer i enkelte av fagsystemene.

I retningslinjen *Tilgangskontroll*, punkt 3.2.3 nr. 10, fremgår det at rutiner for tildeling av tilgang i et system skal utformes av fagansvarlig for systemet. I oversendelsen 31. mai 2023 fremla NAV slike rutiner for fagsystemene PDL-web, Gosys, Infotrygd, Modia og Pesys. Rutinene befinner seg på «Navet». Deltakerne under tilsynet var ikke kjent med om det foreligger rutiner for de øvrige 50 fagsystemene tilsynet omfatter, bortsett fra de som er inntatt i rutinen *Ident- og tilgangsadministrasjon*.

Etter tilsynet gjorde NAV en nærmere undersøkelse av om det finnes flere rutiner. NAV fremla 14. september 2023 et skjermbilde med en forklarende tekst til tilgangen «PESYS/Beregning/Rest/Beholdning». NAV fremla også dokumentet *NAV virksomhetsroller*, versjon 2.11, datert 12. november 2012. Dette dokumentet beskriver de ulike virksomhetsrollene ansatte i NAV kan ha, sortert på type enhet de er ansatt ved. For hver virksomhetsrolle er det blant annet angitt hvilke standardtilganger de ansatte skal ha, og hvilke som er valgfrie. Virksomhetsrollene er ikke systemspesifikke, og gir kun føringer for hvilke tilganger de ansatte skal ha i fellessystemet GOSYS.

NAV beskrev i tilsynet at årsaken til mangelen på rutiner kan være at mange av systemene er små og lite relevante for de fleste enheter, slik at det ikke er funnet hensiktsmessig å utarbeide egne rutiner. I tillegg er det i mange tilfeller enkelt/intuitivt å forstå hva de ulike avkrysningsfeltene innebærer – for eksempel avkrysningsfeltet for den ansattes rolle (typisk «veileder», «saksbehandler» osv.).

NAV forklarte at det i tillegg skal foreligge lokale rutiner for tildeling av tilganger på hvert lokalkontor. Lokalkontorene har stor frihet til å organisere seg på egne måter, ut fra hvilke behov de har. For eksempel er det vanlig at små kontorer har vide tilganger, fordi oppgavene på slike kontor er fordelt på færre personer.

NAV informerte om at det totalt er ca. 1 300 identadministratorer og ca. 200 fagsystemer.

Datatilsynet påpekte under tilsynet at det med opptil 200 fagsystemer og rundt ti mulige avkrysningsfelt for hvert system, blir svært mange valgmuligheter for identadministratorene. De fremlagte rutinene beskriver hvordan, men ikke på hvilke vilkår tilgang skal gis (med unntak av den ettersendte forklaringen til tilgangen «PESYS/Beregning/Rest/Beholdning»).

Representantene for NAV som var tilstede under tilsynet kjente ikke til andre organisatoriske tiltak (i form av opplæring, rutiner, arbeidsinstruks) for identadministratorer enn de ovennevnte. NAV opplyste at opplæring er personavhengig – i den forstand at en ny identadministrator er avhengig av at det er andre identadministratorer på enheten som kan gi opplæring. NAV erkjente at dette er en utfordrende situasjon, og opplyste at dette er en av de sentrale svakhetene som ble påpekt i PwCs modenhetsvurdering fra 2020.

Noen fagsystemer er imidlertid ikke tilgjengelige for «avkryssning». Identadministratorer kan kun bestille tilganger til fagsystemer som hører til den lokale enhetens ansvarsområde. I dette ligger en filtreringsmekanisme som setter grenser for hva en enhetsleder kan bestille tilgang til. Enkelte tilganger krever også ekstra godkjenning fra sikkerhetsseksjonen.

NAV svarte ikke direkte på om identadministratorene har noen kontrollfunksjon overfor enhetsleder, eller om de først og fremst utfører praktiske oppgaver på bestilling fra enhetsleder.

NAVs arkivsystem («Joark») er sentralt for å forstå hvilke personopplysninger som tilgjengeliggjøres for ansatte når de gis tilganger i et fagsystem.

Arkivsystemet er beskrevet på følgende måte på side 11 – 12 i notatet *Tilgangsstyring og logging i NAV*:

«I NAVs fagsystemer lagres primært strukturerte person- og saksopplysninger. Dokumentasjon (brev, vedtak etc.) i PDF-format lagres i Joark, som er NAVs primære fagarkiv.

(...)

En journalpost i Joark tilhører ikke noe spesifikt fagsystem, men kan vises i alle fagsystemer der det er relevant for saksbehandlingen. Det er Joark og ikke fagsystemet som bestemmer hvorvidt journalposten og tilhørende dokumenter kan vises til saksbehandleren. Tilgangsstyringen til dokumenter er derfor lik på tvers av fagsystemer.

De viktigste reglene for tilgangsstyring av journalposter og dokumenter er tilgang til bruker og tema. For å få tilgang til en bruker, sjekkes medarbeiderens roller i AD opp mot brukers egenskaper, som skjerming og adressebeskyttelse. Medarbeideren trenger også tilgang til brukers geografi. I praksis er dette lik tilgang til den NAV-enheten som behandler saker for kommunen som brukeren er folkeregistrert i. Noen fagsystemer organiserer saksbehandlingen i én felles kø for hele landet, og saksbehandlerne som jobber i disse fagsystemene må ha nasjonal tilgang for å få tilgang til brukerne.

Tema på journalposten er også relevant for tilgangsstyringen. Hovedregelen er at medarbeidere i NAV får se journalposter, altså metadata om dokumenter, på alle tema, forutsatt at de har tilgang til brukeren. Medarbeideren trenger imidlertid tematilgang for å kunne åpne selve dokumentet. Dette gjør at medarbeiderne kan få et overblikk over hvilke ytelser og tjenester en bruker har, samtidig som de ikke får innsyn i detaljerte opplysninger utover sitt hovedansvarsområde. (...)»

I det samme notatet har NAV forklart at tema- og enhetstilganger lagres i Axsys. Før tilsynet mottok Datatilsynet detaljert informasjon om 55 fagsystemer. Av denne informasjonen fremgår det at 31 av 55 systemer ikke bruker Axsys. Vi ønsket derfor å få belyst hva dette innebærer for tilgangene i Joark, for eksempel om slike systemer gir landsdekkende tilgang på dokumenter.

Til dette opplyste NAV at Joark ikke henter tema- og enhetstilganger fra Axsys direkte. NAV har i sine merknader i brev 22. november 2023 korrigert dette. NAV opplyser at Joark henter tema- og enhetstilganger fra Axsys og bruker denne informasjonen til sin tilgangskontroll. Tilgangskontrollen for Joark er dermed uavhengig av tilgangskontrollen i fagsystemene. Ifølge NAV sikrer dette korrekt tilgangskontroll til dokumenter, og de vurderer at dette fungerer godt.⁷⁸

Videre opplyste NAV at Joark ikke har noen brukerflate. Det er derfor ikke mulig å gjøre søk direkte i Joark. Tilgangen til Joark går alltid gjennom et fagsystem. Dette har en viss betydning for hvem en kan se metadata om i Joark.

⁷ Endret etter innspill fra NAV 22.11.23.

⁸ Innspill fra NAV 22.11.23: «Det som ikke kom tydelig nok frem i dokumentet “Tilgangsstyring og logging i NAV”, er at selv om Joark teknisk sett gir en saksbehandler tilgang til metadata på alle tema (unntatt KTA [Kontroll anmeldelse] og FAR [Farskap]), filtrerer flere fagsystemer dette resultatet før det presenteres til saksbehandler. For eksempel viser Arena metadata på 14 av 60 tema. Det enkelte fagsystem viser metadata på de tema som er nødvendig for å kunne utføre saksbehandlingen som gjøres der. Hvilke tema hvert enkelte fagsystem viser, er dokumentert i fagsystemets besvarelse.»

5.3.2 Datatilsynets vurdering

Rutiner for og opplæring i hvordan tilganger i praksis skal tildeles er nødvendige tiltak for å sikre at styrende retningslinjer gjennomføres, og for å demonstrere at kravene til personopplysningssikkerhet er ivaretatt.

Gjennomgangen har vist at NAV ikke har organisatoriske tiltak i form av opplæring av identadministratorer. Identadministratorene har enkelte rutiner som gir veiledning om praktisk gjennomføring av tildeling av tilganger i noen av de største fagsystemene. Samtidig er vilkårene for om tilgang skal gis i liten grad definert. Vi ser at virksomhetsrollene i mange tilfeller vil kunne gi veiledning. Identadministratorene vil likevel i mange tilfeller måtte ta beslutninger etter eget skjønn, i fraværet av utfyllende rutiner. Datatilsynets vurdering er derfor at identadministratorene ikke har verktøy som gjør dem i stand til å forvalte myndigheten de er gitt på en betryggende måte. Manglende styring og systematikk gjør det også vanskelig å kontrollere praksisen for den behandlingsansvarlige.

Som NAV selv har beskrevet, har lokalkontorene stor frihet til å organisere tilgangsstyringen på egne måter ut fra hvordan de utøver sine oppgaver. Etter vår vurdering er dette lite tilfredsstillende i en organisasjon som NAV. Det må forventes at NAV har rutiner som etablerer en enhetlig måte å forvalte tilganger på i lokalkontorene.

Samlet sett er vår vurdering at det er et stort behov for å forbedre NAVs rutiner for opplæring og tildeling av tilganger. Kvaliteten på de nåværende rutineene på dette området er ikke forholdsmessige til risikoen ved behandlingen.

Tilgangen til metadata om dokumenter i Joark er etter vårt syn særskilt problematisk. Som NAV har angitt, vil en kunne se metadata om dokumenter i Joark på alle ytelsesområder (unntatt KTA og FAR) i NAV dersom en har tilgang til den registrerte gjennom et fagsystem. Slike metadata kan⁹ inneholde særlige kategorier personopplysninger.¹⁰ Systemer med mange registrerte som mange ansatte har tilgang til, vil derfor medføre en betydelig konfidensialitetsrisiko. Dette er for eksempel tilfellet for fagsystemet Arena, hvor det er ca. 3.7 millioner registrerte og ca. 21 000 ansatte med tilgang til systemet, herunder ca. 15 000 med landsdekkende tilgang.¹¹

Datatilsynet anser dette som uakseptabelt. Ordningen er ikke forenlig med konfidensialitetsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav f og kravene til personopplysningssikkerhet i artikkel 32 nr. 1. NAV har synliggjort at det i mange tilfeller vil være behov for innsyn i ytelser på andre fagområder enn en selv jobber med, fordi ulike

⁹ NAV opplyste 22.11.23 at de har en journalrutine som bl.a. sier "Skriv aldri sensitiv informasjon, personnavn eller fødselsnummer i dokumentbeskrivelsen." NAV mener derfor at det ikke er dekning for å si at metadata i Joark ofte inneholder særlige kategorier personopplysninger. De opplyser at tilfeller der dette forekommer i så fall er brudd på interne rutiner.

¹⁰ Endret etter innspill fra NAV 22.11.23.

¹¹ NAV presiserte 22.11.23 at «[d]et riktige antall ansatte som har tilgang til Arena, er 16 923 (per 21.11.2023). Også for landsdekkende roller har vi oppgitt antall Arena-identer, ikke antall ansatte. Det korrekte er at det er 5 758 ansatte som har landsdekkende tilgang i Arena og 7 240 ansatte som har utvidbar landsdekkende tilgang i Arena (per 21.11.2023). (...) Arena viser frem metadata og dokumenter fra Joark, men bare for temaene som er relevant for saksbehandlingen som utføres der. Arena viser dokumentmetadata på 14 av totalt 60 tema.»

ytelser kan være gjensidig betinget av hverandre. Det må imidlertid etableres tekniske og organisatoriske tiltak som kun tillater innsyn på tvers av fagområder i tilfeller hvor det er nødvendig og det foreligger et faktisk tjenstlig behov.

5.4 Prinsippet «tjenstlig behov» og landsdekkende tilganger

5.4.1 Faktiske forhold

Det følger av retningslinjene for tilgangskontroll og autorisasjon at tilganger til fagsystemene skal gis i henhold til prinsippet NAV betegner som «tjenstlig behov» eller «least privilege». Prinsippet fremstår som det sentrale styringsmålet ved tildeling av tilganger.

Tjenstlig behov defineres ut fra den enkelte medarbeiders arbeidsoppgaver, og tilganger tildeles etter en subjektiv vurdering utført av vedkommendes enhetsleder eller eventuell identadministrator.

Det finnes ingen rutine som beskriver hvordan enhetsleder skal vurdere tjenstlig behov. NAV opplyser at beskrivelser av roller fra arbeids- og tjenesteavdelingen gir en naturlig forståelse av hvilke tilganger som er riktige, og at dette som oftest gir et riktig resultat.

Direktoratet har gjennomført en intern kartlegging av tilganger ved kontorene i Lillestrøm og Skien. Resultatet viste at veiledere ved kontorene normalt hadde 17 – 22 tilganger og at de i praksis hadde vurdert det tjenstlige behovet likt for sine ansatte.

Under tilsynet ble den såkalte køordningen trukket frem. Alle de nyere fagsystemene skal ha en slik ordning. Køen er en liste over oppgaver som er tilgjengelig for saksbehandlere. Av den ettersendte dokumentasjonen fremgår det at køordningen først og fremst er et tiltak for produksjonsstyring, ikke tilgangsstyring.

I systembeskrivelsene NAV har sendt inn i forkant av tilsynet fremgår det at ca. 21 000 ansatte har en lesetilgang i fagsystemet Arena. Under tilsynet ble det opplyst at ca. 16 000 av disse er veiledere. Arena er et eldre system som omfatter flere fagområder. Lesetilgangen er nødvendig for å få tilgang til systemet, men gir ikke alene tilgang til spesifikk informasjon. I Arena har også ca. 15 000 ansatte tilgangen «medisinsk tilgang».¹²

For å få tildelt denne er det også nødvendig å ha tilgangen «sensitiv tilgang saksbehandler», som ca. 17 000 har. I tillegg har opptil ca. 15 000 landsdekkende tilgang (inkludert «utvidbare» tilganger).¹³ NAV begrunner dette med at måten særlig veiledernes arbeid er organisert har endret seg fra å være lokalt basert, til å omfatte hele landet. Dette fører til at flere har tjenstlig behov for flere tilganger, og dermed til store populasjoner. Tidligere var det ikke nødvendig å søke opp brukere bosatt utenfor egen kommune, men den nåværende organiseringen gjør at veilederne har behov for nasjonale tilganger. Tilgangsmodellen som

¹² Se fotnote 11.

¹³ Se fotnote 11.

fremgår av retningslinjen *Tilgangskontroll og Autorisasjon* passer dermed ikke lenger til måten NAV er organisert på.

I forkant av tilsynet merket Datatilsynet seg at enkelte systemer hadde såkalte «utvidbare» roller, særlig avgrenset etter geografi, men også etter andre kriterier. NAVs oppfatning var at disse rollene ikke lenger har særlig relevans. De utvidbare rollene ble utfaset i Gosys i perioden etter at dokumentasjonen for systemene ble sendt til oss, men de eksisterer fortsatt i Arena.

NAVs deltakere under tilsynet kunne ikke si om det finnes en rutine for når og hvordan rollene skal brukes, men dette kan foreligge hos produktteamene. Vurderingen av når de utvidbare rollene skal brukes er overlatt til den enkelte ansatte. Bruken av utvidbare roller krever at den ansatte skriftlig begrunner nødvendigheten. NAV opplyste under tilsynet at deres erfaring er at disse begrunnelsene ikke har særlig nytteverdi i vurderingen av om disse tilgangene brukes riktig.

NAV fremholdt under tilsynet at tidsbegrensede tilganger ville vært en bedre løsning.

Det fremgår av systembeskrivelsene at Bisys, som brukes i bidragssaker, har ca. 2 millioner registrerte. Dette foranlediget spørsmål om i hvilken utstrekning ansatte har tilgang til historiske saker. I den ettersendte dokumentasjonen opplyser NAV at NAVs fagsystemer er arkiv etter arkivloven. Saker overføres derfor ikke til arkiv utenfor fagsystemene. Alle saker, både aktive og inaktive, er tilgjengelige for saksbehandler i tråd med vedkommendes tilgangsrettigheter. I henhold til NAVs bevarings- og kassasjonsplan skal dokumentasjonen i fagsystemer avleveres til Arkivverket etter at NAV ikke lenger har behov for den.

5.4.2 Datatilsynets vurdering

Det fremstår klart for Datatilsynet at NAVs holdning er at tjenstlig behov som prinsipp er viktig. Vi mener likevel at måten organiseringen og gjennomføringen av arbeidsoppgavene i NAV har utviklet seg har gjort det vanskelig å begrense tilganger i praksis, og at tjenstlig behov-prinsippet ikke er et egnet styringsmål. Store systemer som brukes på flere områder (f.eks. Arena og Gosys) gjør at en betydelig andel av brukerne har et tjenstlig behov for vide tilganger.

Videre vurderer Datatilsynet at rutinene for tildeling av tilganger er utdaterte og gamle, og at de ikke er relevante sett opp mot til dagens organisering av NAV. Eksempelvis fremgår det under tilsynet at praksisen med utvidbare landtilganger ikke lenger kan brukes som forutsatt. Rutinene som er knyttet opp mot disse utvidbare rollene er dermed heller ikke hensiktsmessige.

Rutinene som er rettet mot identadministratorer gir ingen veiledning knyttet til skjønnsvurderingene ved tildelingen av tilganger, og det er overlatt til den enkelte enhet å ta stilling til hvilke tilganger som er riktige. Manglende rutiner ved tildeling av tilganger gjør det også vanskelig å føre kontroll med om praksisen skjer i tråd med prinsippet om tjenstlig behov.

Køordningen som ble trukket frem under tilsynet har ikke tilgangsstyring som formål, men er et verktøy for produksjonsstyring. Datatilsynet ser imidlertid at denne ordningen kan bidra til å knytte oppslag til aktuelt tjenstlig behov ved etterkontroll. NAV opplyste at denne muligheten ikke brukes i dag.

Datatilsynet tar til etterretning at NAVs fagsystemer også fungerer som arkiv i henhold til arkivloven. Vi mener samtidig at det er behov for å utarbeide tiltak for å begrense tilgangen til opplysninger om personer som ikke har noen aktive saker hos NAV. Det er ikke en tilfredsstillende situasjon at alle historiske saker ligger åpne. Det gjelder særlig overfor registrerte personer som ikke har noen aktive saker som kan gi utspring til et aktuelt tjenstlig behov. Ordningen anses ikke forenlig med konfidensialitetsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav f og kravene til personopplysningssikkerhet i artikkel 32 nr. 1.

Den interne undersøkelsen av tilgangene for veiledere på kontorene i Lillestrøm og Skien viste at en forholdsvis lik linje for antall tilganger følges i praksis. Datatilsynet mener at nødvendigheten av å manuelt måtte undersøke enkeltkontor for å få oversikt over tildelte tilganger viser mangler i styringssystemet til NAV. Manglende overordnede rutiner gjør at resultatet fremstår som mer tilfeldig enn som resultatet av gode prosesser og styring.

5.5 Beskyttelse av personer med fortrolig og strengt fortrolig adresse

5.5.1 Faktiske forhold

Trusselutsatte personer kan få innvilget vedtak om adressesperre, jf. folkeregisterloven § 10-4 jf. beskyttelsesinstruksen § 3, jf. § 4. Beskyttelsesinstruksen har graderingene «strengt fortrolig» og «fortrolig», jf. beskyttelsesinstruksen § 4. Dette omtales gjerne som adressesperre kode 6 og 7.

NAV har ikke tilgang til selve adressen til de som lever på strengt fortrolig adresse (kode 6). Disse adressene skal håndteres av Kripos. [REDACTED]

I tillegg til de som lever på adressesperre i Norge, har NAV noen registrerte som bor på strengt fortrolig adresse i utlandet. Disse adressesperrene er ikke registrert i Folkeregistret, og NAV er avhengig av å få denne informasjonen fra andre kilder, i hovedsak via utenlandske myndigheter. Det er få ytelser som omfatter denne gruppen. NAV opplyste at gruppen består av ca. 50 personer.

Iverksettelse av en adressesperre foretas av politiet og innebærer at all informasjon som kan si noe om hvor den trusselutsatte oppholder seg, såkalt geolokaliserende informasjon, er gradert. Hvilke opplysninger som kan sies å være geolokaliserende, må vurderes konkret i hvert enkelt tilfelle.

I notatet *Tilgangsstyring og logging i NAV* beskriver NAV hvordan tilgang til opplysninger om personer med fortrolig eller strengt fortrolig adresse begrenses i deres fagsystemer. Saker

knyttet til personer i denne gruppen behandles ved et virtuelt kontor med særskilt oppnevnte saksbehandlere.

Det er totalt ca. [redacted] ansatte i NAV som har tilgang til opplysninger om personer i denne gruppen. [redacted] NAV begrunnet dette med hensynet til likebehandling og kvaliteten på tjenesten. NAV opplyser at de har erfaring med at denne gruppen ikke har fått samme kvalitet på saksbehandlingen som resten av befolkningen når det har vært færre med tilgang og mulighet for å følge de opp.

5.5.2 Datatilsynets vurdering

Risikoen ved å behandle opplysninger om personer med fortrolig og strengt fortrolig adresse er ekstraordinært høy. Dette innebærer krav til særskilte tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet for denne gruppen, jf. personvernforordningen artikkel 32.

NAV har utarbeidet en rekke tekniske og organisatoriske tiltak for å beskytte informasjon om både de med fortrolig og strengt fortrolig adresse, samt rutiner som gjelder ansatte som jobber med denne gruppen særskilt. NAV har demonstrert etterlevelse gjennom oversendte rutiner.¹⁴

Datatilsynet anser at antallet ansatte med tilgang til denne brukergruppen er forholdsvis høyt.

[redacted]
[redacted] Antall ansatte som har tilgang kan derfor fremstå høyt, men vi har ikke under tilsynet undersøkt nærmere om tilgangene faktisk er begrunnet i tjenstlig behov i de ulike fagsystemene.

Datatilsynet anser de tekniske og organisatoriske tiltakene for beskyttelse av personer med fortrolig eller strengt fortrolig adresse som tilstrekkelige og egnede.

Vi legger til grunn at NAV gjennomgår relevante rutiner, og at tilgangene jevnlig revideres slik at ikke flere enn nødvendig har tilgang til opplysninger om personer i denne gruppen.

5.6 Beskyttelse av egne ansatte

5.6.1 Faktiske forhold

Ansatte i NAV kan også ha rett på ytelser fra NAV. Som nevnt ovenfor, har NAV mer enn 20 000 ansatte. Det er utarbeidet særskilte rutiner for tekniske og organisatoriske tiltak for å beskytte informasjonen til egne ansatte og deres nærstående.

NAV har siden 2018 etablert nye løsninger for å skjerme egne ansatte. Opplysninger om ansatte blir automatisk sperret fra de generelle tilgangene, og det er etablert virtuelle kontorer for saksbehandling og oppfølging. De ansattes familiemedlemmer eller nære kan også få

¹⁴ Disse rutinene er unntatt offentlighet, og er derfor ikke gjengitt.

tilsvarende beskyttelse. Skjerming av egne ansatte skjer automatisk, mens nærmeste familie eller andre med nær relasjon til den ansatte kan be om skjerming via nav.no.

Behovet for skjerming er varierende blant de ansatte, og sperrene kan oppheves ved ønske.

Saksbehandlere som behandler ansattes saker er organisert i virtuelle enheter. Oppgaver rutes til disse enhetene istedenfor de vanlige saksbehandlingsenhetene. Kun ansatte med særskilt tilgang kan se data og saksbehandle denne gruppen. De virtuelle kontorene har egne enhetsledere. Løsningen ble utviklet i prosjektet «Logginnsyn og ansatte som brukere» i 2019-2020.

Antall ansatte med tilgang til ulike fagsystemer varierer. For eksempel er det 249 som har tilgang til ansatte i Arena, mens 5 ansatte har en utvidbarrolle som kan gi midlertidig tilgang til denne gruppen. Til sammenligning er det 870 som har tilgang til sykefraværsoppfølging av egne ansatte i Modia. 867 har tilgang til egne ansatte via GOSYS og 870 i nEESSI.¹⁵

5.6.2 Datatilsynets vurdering

Datatilsynet vurderer, i liket med NAV, at ansatte i NAV bør ha et særskilt konfidensialitetsvern. Risikoen for at behandling av opplysninger om ansatte kan ha negative følger for den ansattes rettigheter og friheter må anses som høyere enn i normale tilfeller, noe som påkrever konkrete vurderinger av hva som vil være egnede tekniske og organisatoriske tiltak.

Datatilsynet har også tidligere vurdert NAVs evne til å skjerme egne ansatte. Datatilsynet legger til grunn NAVs vurdering av at løsningen er hensiktsmessig og tilstrekkelig. Vi vil vurdere ordningen etter at den har vært i bruk over en periode. Dette temaet følges opp i sak 21/04141.

5.7 Andre grupper med særskilt behov for konfidensialitetsvern

5.7.1 Faktiske forhold

Det gikk frem under tilsynet at det ikke foreligger noen særskilte tekniske eller organisatoriske tiltak for skjerming av andre grupper enn de som er omtalt over. Det medfører at registrerte som av andre grunner har et særskilt behov for konfidensialitetsvern, f.eks. offentlig eksponerte personer, ikke kan få det. NAV anser at sikkerheten generelt i NAV gir et tilstrekkelig vern for denne gruppen.

NAV fremholdt under tilsynet at det er vanskelig å definere hvilke grupper som har særskilte behov, for eksempel hvem som skal regnes som en offentlig eksponert person.

¹⁵ NAV presiserte 22.11.23 følgende: «For å få tilgang til egne ansatte i et system må saksbehandler ha både tilgang til fagsystemet og tilgangen «egen ansatt» og dette kom trolig ikke godt nok fram i vår oversendelse. De riktige tallene for egen ansatt på de nevnte områdene er:

- Antall ansatte med egen ansatt og sykefraværsoppfølging: 276
- Antall ansatte med egen ansatt og nEESSI: 192
- Antall ansatte med egen ansatt og Gosys: 867»

5.7.2 Datatilsynets vurdering

Datatilsynet støtter at det viktigste må være at tilgangsstyringen i NAV generelt er god. Samtidig vurderer vi at tilgangene i NAV generelt er vide. Datatilsynet mener derfor at flere bør ha mulighet til å oppnå et særskilt konfidensialitetsvern, basert på individuelle behov. Vurderingen av hvilke tiltak som er egnede og tilstrekkelige må gjøres for konkrete tilfeller. Skjerming gjennom dedikerte saksbehandlere eller kontorer vil trolig være egnet i mange tilfeller.

Vi har forståelse for at det kan være vanskelig å utforme kriterier for hvem som skal kvalifisere til et særskilt vern. Som et minimum bør NAV innføre skjermingstiltak for brukere som uttrykker et ønske om det og har en saklig grunn. Kriterier for vurderingen og hvilke tekniske tiltak som bør iverksettes bør fremgå av en konkret rutine, og beslutninger bør kunne kontrolleres.

NAVs manglende tekniske og organisatoriske tiltak for skjerming begrunnet i konkrete brukerbehov anses som et avvik fra kravet om at personopplysningssikkerheten er tilpasset risikoen ved behandlingen, jf. personvernforordningen artikkel 32 nr. 1 og 2.

5.8 Revisjon

5.8.1 Faktiske forhold

På side 4 i notatet *Tilgangsstyring og logging i NAV* fremgår det at alle enhetsledere skal revidere tilgangene til sine ansatte minst en gang i året.

Under tilsynet undersøkte Datatilsynet hvilke hjelpemidler enhetslederne har til rådighet når de skal gjøre denne oppgaven. NAV opplyste at enhetslederne kan hente ut rapporter fra Identrutina med lister over hvilke tilganger de ansatte har. Enhetslederne må deretter sjekke om tilgangene korresponderer med de ansattes oppgaver. For Arena er rapporten fra Identrutina imidlertid ikke dekkende. Tilganger i Arena må sjekkes separat.

NAV uttalte under tilsynet at de ser at det er behov for å forbedre enhetsledernes støtteverktøy på dette området.

Når det gjelder Joark, er tilgangskontrollen implementert i systemet. Men tilgangsstyringen til Joark fungerer på samme måte for Joark som for andre systemer i NAV. Identrutina brukes for å gi tilgang til tema, enheter, geografi (nasjonal og regional tilgang) og andre tilganger Joark benytter for å gi tilgang til dokumenter og metadata. Disse tilgangene revideres av enhetsleder på linje med andre tilganger. I praksis er det dermed slik at enhetsledere reviderer tilganger til Joark.¹⁶

¹⁶ Endret etter innspill fra NAV 22.11.23.

Det er ikke etablert noen standardisert metode for enhetslederne til å dokumentere at den årlige revisjonen er gjennomført, men det er mulig for enhetsleder å få en kvittering fra Identrutina. Dokumentasjonen varierer fra enhet til enhet.

Ved bytte av avdeling e.l. slettes alle tilganger og legges inn på nytt.

Datatsynet ønsket å belyse hvordan NAV gjennom sitt styringssystem sikrer at enhetslederne gjennomfører den årlige revisjonen («revisjon av revisjonen»), og om NAV kontrollerer at enhetslederne praktiserer tildelinger korrekt.

NAV opplyste at det finnes en egen rutine for å påse at enhetsledere gjennomfører årlig revisjon. Denne ble ettersendt 14. september 2023 (dokumentet *Brukeridenter og tilgangsrettigheter – rutiner for administrasjon*, versjon 1.2, datert 18. juni 2020). I rutinen stilles det tydelig krav til at enhetsleder gjennomfører årlig revisjon av tilganger. Rutinen besvarer imidlertid ikke spørsmålet om det foretas noen kontroll av om revisjon er gjennomført. Det fremgår likevel på side 3 i *Standard for tilgangsforvaltning* at produktledere (ansvarlig for egne fagsystem) har ansvar for periodisk gjennomgang av tilganger.

Når det gjelder enhetsledernes kompetanse, opplyste NAV at det gjøres stikkprøver basert på sammenlignende analyser. NAV informerte også om at de har jevnlig møter med identadministratorene. Denne dialogen klargjør misforståelser. Datatsynet har ikke blitt presentert for noe dokumentasjon som bekrefter disse rutinene.

5.8.2 Datatsynets vurdering

Kravene til revisjon av tilganger er i seg selv et nødvendig sikkerhetstiltak etter personvernforordningen artikkel 32 nr. 1, men kan også knyttes spesifikt til artikkel 32 nr. 1 bokstav d.

Datatsynet vurderer at NAVs praksis med årlige revisjoner er et akseptabelt intervall. Enhetslederne har imidlertid ikke rutiner som understøtter denne oppgaven. Hverken gjennomførende eller kontrollerende rutiner er etablert. Dette har etter vårt syn sammenheng med at rutinene for tildeling av tilganger i utgangspunktet er mangelfulle, jf. omtalen under punkt 5.5.2. Som påpekt der, gjør manglende rutiner ved tildeling av tilganger det vanskelig å føre kontroll med om praksisen skjer i tråd med prinsippet om tjenstlig behov.

NAV har rundt 400 enhetsledere som er gitt stor frihet og stort ansvar uten et tydelig rammeverk å forholde seg til. Behovet for en overordnet kontroll med tilgangsforvaltningen er derfor tydelig.

NAV har beskrevet at det foretas stikkprøver av enhetsledernes praksis som er basert på sammenlignende analyser. Datatsynet vurderer at kontroll av hvordan revisjon gjennomføres må foretas rutinemessig og forankres i NAVs styringssystem.

Vi merker oss at produktledere skal foreta periodisk gjennomgang av tilganger. Dette temaet ble ikke nærmere belyst i tilsynet, og Datatsynet vil derfor ikke vurdere hvordan dette virker inn på revisjonen av enhetsledernes praksis.

Vi påpeker at også produktledernes gjennomgang bør forankres i styringssystemet og sikres gjennom rutiner.

5.9 Oppsummering og konklusjon

Datatilsynet har konstatert følgende avvik knyttet til tilgangsstyring:

- **Avvik 2:** NAVs styrende dokumentasjon for tilgangsstyring mangler egnede tekniske og organisatoriske tiltak for å sikre og påvise at deres behandling av personopplysninger utføres i samsvar med personvernforordningen, jf. artikkel 32 nr. 1 og 2, jf. også artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2. Se punkt 5.2.
- **Avvik 3:** NAVs styrende dokumentasjon for tilgangsstyring er ikke gjenstand for regelmessig revisjon i henhold til kravene i personvernforordningen artikkel 32 nr. 1 bokstav d. Se punkt 5.2.
- **Avvik 4:** NAV har ikke etablert tilfredsstillende organisatoriske tiltak for å sikre at det gjennomføres risikovurderinger i henhold til personvernforordningen artikkel 32 nr. 2 ved etablering og utvikling av fagsystemer. Se punkt 5.2.
- **Avvik 5:** Tilgjengeliggjøringen av metadata om dokumenter i Joark er for generell og vid og er ikke forenlig med konfidensialitetsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav f og kravene til personopplysningssikkerhet i artikkel 32 nr. 1. Se punkt 5.3.
- **Avvik 6:** NAV har ikke etablert tilfredsstillende organisatoriske tiltak for opplæring av identadministratorer. Konklusjonen vår er at dette er et avvik fra kravene i personvernforordningen artikkel 32 nr. 1. og nr. 4. Se punkt 5.3 og 5.4.
- **Avvik 7:** Rutinene for tildeling av tilganger er utdaterte og gir ingen veiledning knyttet til skjønsmessige vurderinger. Dette er å regne som et avvik fra kravene til organisatoriske tiltak etter personvernforordningen artikkel 32 nr. 1 og nr. 4. Se punkt 5.4.
- **Avvik 8:** Tilgjengeliggjøringen av personopplysninger som kun behandles for arkivformål (historiske saker) er for generell og vid og er ikke forenlig med konfidensialitetsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav f og kravene til personopplysningssikkerhet i artikkel 32 nr. 1. Se punkt 5.4.
- **Avvik 9:** NAV har organisert seg på en måte som gjør at en betydelig andel av brukerne får et tjenstlig behov for å ha vide tilganger. I kombinasjon med et mangelfullt system for loggkontroll (se punkt 7 nedenfor) er dette ikke forenlig med konfidensialitetsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav f og kravene til personopplysningssikkerhet i artikkel 32 nr. 1. Se punkt 5.4.

- **Avvik 10:** NAVs manglende tekniske og organisatoriske tiltak for skjerming begrunnet i individuelle behov er et avvik fra kravet om at sikkerhetstiltak tilpasses risikoen ved behandlingen, jf. personvernforordningen artikkel 32 nr. 1 og 2. Se punkt 5.7.
- **Avvik 11:** NAV har ikke etablert tilfredsstillende rutiner for kontroll av enhetslederens årlige revisjon av tilganger. Dette er et avvik fra kravet i personvernforordningen artikkel 32 nr. 1 bokstav d. Se punkt 5.8.

6 Logg

6.1 Rettslig grunnlag

Logging av aktiviteter i IT-systemene er et nødvendig element i sikkerhetstiltakene som er påkrevd etter personvernforordningen artikkel 32. Vi viser til omtalen av dette under punkt 5.1.

Loggdata bidrar til å oppdage og forebygge uautorisert og ulovlig bruk, og til å kontrollere om sikkerhetstiltakene knyttet til tilgangsstyring har ønsket effekt. Slike kontroller er påkrevd etter artikkel 32 nr. 1 bokstav d.

Etter artikkel 32 nr. 4 skal det treffes tiltak for å sikre at ansatte kun behandler personopplysninger «etter instruks» fra behandlingsansvarlig. Artikkel 24 krever at den behandlingsansvarlige er i stand til å «påvise» at de ovennevnte reglene overholdes. Logging er et viktig instrument for å sikre og demonstrere etterlevelse av regelverket.

6.2 Faktiske forhold

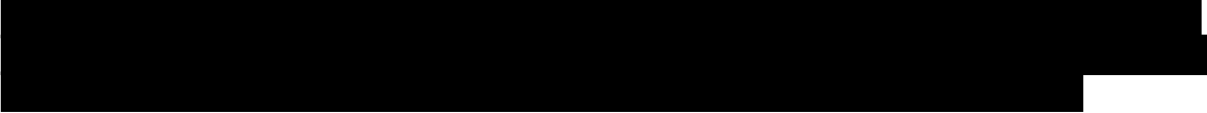
NAV har opplyst at alle oppslag i fagsystemene logges. Åpning av dokumenter logges via Joark. NAV har ulike formål med loggen; verifisering av autorisert bruk og avdekking av uautorisert bruk.

NAV har en overordnet retningslinje for logging av oppslag, som er tilgjengelig på Navet, *Retningslinje om uberettigede oppslag i saksbehandlingssystemene.*

NAV bruker ArcSight-plattformen for lagring og analyse av auditlogger. Alle fagsystemene i NAV skal auditlogge, og loggene sendes til ArcSight via ulike transportmekanismer. Kun to personer i NAV har tilgang til ArcSight.

NAV forklarte under tilsynet at det ikke er noen direkte sammenheng mellom nivået av logging og nivået av tilganger. Loggnivået er konstant og påvirker ikke avgjørelser om hvilke tilganger som kan gis. Dette er to uavhengige prosesser som først ses i sammenheng ved en eventuell etterfølgende undersøkelse av om en tilgang er brukt ulovlig.

NAV opplever at loggene i praksis har vært effektive for å avdekke uberettigede oppslag i fagsystemene. For sikkerhetskopiering og gjenoppretting av loggdata ved systemfeil eller datatap, har NAV etablert rutiner for back-up av alle produksjonssystemer.



NAV gjennomførte en evaluering i 2022, og konkluderte med behov for å erstatte den eksisterende loggløsningen. NAV opplyser at den tekniske loggløsningen oppfattes som tungvint av utviklere som bruker den. Det er behov for å forbedre dokumentasjonen samt retningslinjer og rutiner. Forbedret dokumentasjon inkluderer økt kvalitet på loggdata, mer enhetlig logging, felles terminologi og standardiserte regler for å øke lesbarheten av loggrapportene.

6.3 Datatilsynets vurdering

NAV opplyste under tilsynet at alle oppslag i deres systemer logges. Datatilsynet vurderer at loggene fremstår som egnet til å oppfylle de sentrale funksjonene de skal ha som sikkerhetstiltak.

Logg som teknisk tiltak for å kunne forebygge og oppdage uautorisert og ulovlig bruk og dokumentere etterlevelse av regelverket anses som etablert.

6.4 Oppsummering og konklusjon

Datatilsynet avdekket ikke avvik knyttet til logging under tilsynet.

7 Loggkontroll

7.1 Rettslig grunnlag

Det følger av personvernforordningen artikkel 32 nr. 1 bokstav d at den behandlingsansvarlige skal etablere «en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er».

Kontroll av logger er et sentralt virkemiddel for testing av om sikkerhetstiltakene knyttet til tilgangsstyring er tilstrekkelige og virker etter sin hensikt.

Krav til omfanget av loggkontrollen må vurderes i lys av andre tekniske og organisatoriske tiltak, som til sammen skal være «egnet» med hensyn til risikoen ved behandlingen, jf. artikkel 32 nr. 1 og 2. Snevre tilganger vil ikke gi samme behov for kontroll av faktisk bruk som vide tilganger.

7.2 Faktiske forhold

NAV har ikke etablert noen former for automatisk loggkontroll. Det foreligger heller ingen rutiner for stikkprøvekontroll. Loggkontroll gjøres kun ved forespørsler fra den registrerte eller ved konkret mistanke om at det er gjort oppslag uten tjenstlig behov. NAV har etablert rutiner for fremgangsmåten i disse tilfellene som er fremlagt i dokumentet *Retningslinjer uberettigede oppslag i saksbehandlingssystemene*. Det foreligger ikke egne kontrolltiltak knyttet til oppslag på personer med særskilt behov for konfidensialitetsvern.

NAV gir registrerte personer innsyn i logg. Dette gjør at den registrerte selv kan kontrollere oppslag. I notatet *Tilgangsstyring og logging i NAV* er prosessen for logginnsyn forklart slik på side 10:

«Når en bruker har bedt om logginnsyn, vil Sikkerhetsseksjonen i NAV bestille en innsynsrapport fra ArcSight-administratorene. Rapporten gir en oversikt over oppslag som er gjort på brukeren, og inkluderer tidspunktet, hvilket fagsystem som ble brukt, hvilken NAV-enhet som gjorde oppslaget, og navnet på den NAV-ansatte som gjorde oppslaget. Dersom brukeren ønsker mer informasjon om oppslag etter å ha mottatt innsynsrapporten, kan han eller hun sende en ny henvendelse til Sikkerhetsseksjonen med spørsmål om konkrete oppslag.»

Ved undersøkelsessaker vil Sikkerhetsseksjonen gjennomføre en uavhengig vurdering av de loggoppslagene brukeren ber om. Sikkerhetsseksjonen kontakter da relevante NAV-kontorer, fylkeskontorene eller avdelinger i direktoratet hvor oppslagene har blitt utført, og ber om en nærmere redegjørelse for årsaken til oppslagene og hvilken rolle/funksjon medarbeideren som utførte loggoppslaget, hadde. Basert på redegjørelsen vil Sikkerhetsseksjonen vurdere om loggoppslagene var gjort med tjenstlig behov eller ikke.»

NAV anser at logginnsyn for de registrerte har en preventiv effekt, da saksbehandlere i NAV har høy bevissthet om at oppslag blir synlig overfor den registrerte. NAV opplyste at det har vært færre tilfeller av urettmessige oppslag etter at logginnsyn ble innført.

Når det gjelder revisjon av tilgangsstyringen, informerte NAV under tilsynet om at de anser det mer effektivt å analysere hvilke tilganger medarbeidere faktisk har, enn å basere revisjonen på loggdata. NAV påpekte samtidig at det er en utfordring at mye av styringen er overlatt til lokale NAV-kontor, som har betydelig frihet til å organisere seg på egne måter.

Krav til skriftlig begrunnelse for å benytte utvidbare tilganger er utfaset. NAVs erfaring er at slike begrunnelser ikke er et hensiktsmessig tiltak, fordi det genererer mye tekst av lav kvalitet som er vanskelig å kontrollere i etterkant.

Under tilsynet poengterte NAV at det kan utledes mye informasjon fra tekniske spor i selve fagsystemene som kan bidra til å belyse om oppslag har vært berettiget. NAV opplyste at det er enhetsledernes oppgave å undersøke slike spor, og at dette fremgår av standardbrevet Sikkerhetsseksjonen sender enhetsleder i forbindelse med undersøkelsessaker. Dette standardbrevet ble fremlagt for Datatilsynet i ettersendelsen 14. september 2023. Datatilsynet kan ikke se at brevet gir enhetsleder noen instruks om å undersøke tekniske spor i fagsystemene.

7.3 Datatilsynets vurdering

Som påpekt i punkt 5.4.2 ovenfor, har NAV organisert seg på en måte som har gjort det vanskelig å begrense tilganger i praksis, og en betydelig andel av brukerne får et tjenstlig behov for å ha vide tilganger. Dette medfører et skjerpet krav til loggkontroll.

NAV har ikke etablert systematisk kontroll av loggene i sikkerhetsarbeidet for å avdekke uberettigede oppslag. Datatilsynets vurdering er at NAVs styringsprinsipp om tjenstlig behov ikke vil kunne kontrolleres uten systematisk gjennomgang av logger.

Med hensyn til arten og omfanget av NAVs behandling av personopplysninger, i kombinasjon med manglende rutiner for tildeling av tilganger, vurderer Datatilsynet at det ikke er tilfredsstillende at loggkontrollen er begrenset til manuelle undersøkelser som det i hovedsak er opp til den registrerte å ta initiativ til. Det er positivt at NAV gir de registrerte innsyn i loggen, men dette kan ikke anses som et sikkerhetstiltak etter personvernforordningen artikkel 32.

Datatilsynet vurderer på denne bakgrunnen at NAVs tekniske og organisatoriske tiltak for loggkontroll ikke i tilstrekkelig grad gir egnede tekniske og organisatoriske tiltak for å sikre og påvise at deres behandling av personopplysninger utføres i samsvar med personvernforordningen, jf. artikkel 24 nr. 1 og artikkel 32 nr. 1 og 2. At det ikke er etablert noen systematisk loggkontroll avviker også fra kravene til regelmessig kontroll etter artikkel 32 nr. 1 bokstav d.

7.4 Oppsummering og konklusjon

Datatilsynet har konstatert følgende avvik knyttet til loggkontroll:

- **Avvik 12:** NAV har ikke etablert en systematisk loggkontroll. I kombinasjon med at en betydelig andel av NAVs ansatte har vide tilganger (se punkt 5.4/avvik 9 ovenfor), blir dette å regne som et avvik fra kravet om å innføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen, jf. artikkel 32 nr. 1 og 2, jf. også artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2, og fra kravene til regelmessig kontroll etter artikkel 32 nr. 1 bokstav d.