

ARBEIDS- OG VELFERDSETATEN
Postboks 354
8601 MO I RANA

Deres referanse
23/4873-21

Vår referanse
23/00708-28

Dato
18.03.2024

Vedtak om pålegg og overtredelsesgebyr

Innholdsfortegnelse

1.	Innledning.....	2
2.	Oppsummering	3
3.	NAVs kommentarer til varsel om vedtak.....	4
4.	Vedtak om pålegg.....	5
5.	Frister for gjennomføring	7
6.	Vedtak om ileggelse av overtredelsesgebyr	7
7.	Tilsynets omfang og sakens opplysning.....	8
7.1	Omfang	8
7.2	Opplysning av saken.....	8
8.	Personvern i NAV	12
9.	Hovedfunn i det stedlige tilsynet.....	13
10.	Tidligere tilsyn og evalueringer mv. av NAV	15
10.1	Tilsyn i 2007	15
10.2	Tilsyn i 2010	16
10.3	Tilsyn i 2011	16
10.4	BDO og Wiersholms evaluering av NAV i 2016	17
10.5	PwCs evaluering av NAV i 2020.....	17
10.6	NOU 2023: 11 – Raskt og riktig	17
10.7	Avsluttende merknad – tidligere tilsyns betydning for denne saken	17
11.	Datatilsynets vurdering av NAVs tilsvare og begrunnelse for vedtak om pålegg	18

11.1	Innledning	18
11.2	Pålegg 1 – Etablere et helhetlig og egnet styringssystem	18
11.3	Pålegg 2 – Tilgangsstyring.....	25
11.4	Pålegg 3 – Logg og loggkontroll	29
12.	Innledende om overtredelsesgebyr.....	30
12.1	NAVs kommentarer til varsel om overtredelsesgebyr.....	30
12.2	Generelt om overtredelsesgebyr	30
13.	Vurdering av om overtredelsesgebyr skal ilegges.....	31
13.1	Lovkravet	31
13.2	Konkurrens.....	32
13.3	Skyldkravet	33
13.4	Vurderingsmomenter som skal tillegges særlig vekt	35
13.5	Utmåling av gebyret.....	41
14.	Klageadgang.....	43
15.	Innsyn og offentlighet	43

1. Innledning

Vi viser til det stedlige tilsynet Datatilsynet gjennomførte hos Arbeids- og velferdsetaten (NAV) 6. september 2023.

Endelig tilsynsrapport og varsel om vedtak ble oversendt NAV 27. november 2023. NAV ga sine merknader til de varslede vedtakene 4. januar 2024. Fristen for å gi kommentarer var opprinnelig 18. desember 2023, men ble forlenget til 4. januar 2024 etter anmodning fra NAV 12. desember 2023.

Tilsynet ble gjennomført med hjemmel i personvernforordningen artikkel 57 nr. 1 bokstav a og bokstav h, jf. artikkel 58 nr. 1 bokstav a, b, e og f. Personvernforordningen er gjennomført i norsk rett ved inkorporasjon, se personopplysningsloven § 1.

Det fremgår av personopplysningsloven § 20 at Datatilsynet er tilsynsmyndighet etter personvernforordningen artikkel 51.

Hjemlene våre for å gi pålegg og å ilegge overtredelsesgebyr er henholdsvis personvernforordningen artikkel 58 nr. 2 bokstav d og artikkel 58 nr. 2 bokstav i. Vi viser også til personopplysningsloven § 26 andre ledd, som slår fast at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83.

2. Oppsummering

I tilsynet har Datatilsynet kontrollert om NAV sikrer tilfredsstillende konfidensialitet i IT-løsningene («fagsystemene») som benyttes til å behandle personopplysninger i forbindelse med tjenesteyting. Kontrollen var avgrenset til tekniske og organisatoriske tiltak knyttet til tilgangsstyring, logg og loggkontroll, jf. personvernforordningen artikkel 32 og artikkel 5 nr. 1 bokstav f, herunder om NAV har etablert et egnet styringssystem, jf. personvernforordningen artikkel 24 og artikkel 5 nr. 2.

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

Våre hovedkonklusjoner er at NAVs styringssystem ikke er egnet for å sikre et tilfredsstillende sikkerhetsnivå for personopplysninger, og at konfidensialitetssikringen i NAVs fagsystemer, innenfor ovennevnte avgrensninger, i praksis ikke er tilfredsstillende.

Tilsynet har avdekket en rekke lovbrudd som etter Datatilsynets oppfatning viser strukturelle, organisatoriske svakheter og en manglende styring av og forståelse for betydningen av personvern og hvilke krav som må stilles til NAV på dette området. Vi mener at lovbruddene viser at arbeidet med personopplysningssikkerhet ikke er gitt tilstrekkelig prioritet og ressurser av ledelsen i NAV.

Slik NAVs styringssystem knyttet til tilgangsstyring og loggkontroll er innrettet i dag, er det svært krevende å etterprøve om bruken av fagsystemene skjer innenfor lovens rammer. Lokale kontorer er gitt stor frihet til å organisere seg på egne måter. Det medfører at NAVs styringsprinsipp om «tjenstlig behov» i praksis defineres langt nede i organisasjonen. Det fører til at ledelsen tilsynelatende i stor grad har fraskrevet seg både ansvaret for og muligheten til å kontrollere etterlevelsen av personvernforordningen i praksis. Manglende styring medfører en høy risiko for at etterlevelse beror på tilfeldigheter. Det er ikke akseptabelt for en myndighet som NAV.

I tilsynsrapporten konstaterte vi 12 lovbrudd (i rapporten og i vedtaket her også omtalt som «avvik»). I NAVs brev av 4. januar 2024 er det fremlagt nye opplysninger som gjør at ett av disse bortfaller. NAV pålegges å rette opp de resterende lovbruddene. Datatilsynet har delt lovbruddene i tre overordnede kategorier: styringssystem (pålegg 1), tilgangsstyring (pålegg 2) og loggkontroll (pålegg 3). Vi har lagt NAVs tiltaksplan til grunn for oppfyllelsesfristene vi har satt.

Vi har videre kommet til at NAV også skal ilegges et overtredelsesgebyr som følge av lovbruddene.

Vi viser også til vurderingene våre, og til beskrivelsene av de faktiske og rettslige forholdene i saken, slik de er omtalt i den endelige tilsynsrapporten. Tilsynsrapporten følger vedlagt.

3. NAVs kommentarer til varsel om vedtak

I tilsvaret av 4. januar 2024 skriver NAV innledningsvis at det er viktig for dem å presisere at de «i stor grad er enig i avvikene» som ligger til grunn for de varslede vedtakene, og at «disse må håndteres». NAV har utarbeidet en tiltaksplan for å rette lovbruddene og oppfylle varslede pålegg (del II av tilsvaret). NAVs øvrige merknader fremgår i del I av tilsvaret.

Følgende tiltak og frister er foreslått av NAV i tilsvaret:

Nr.	Tiltak	Frist
1	Oppdatere den styrende dokumentasjonen for tilgangsstyring, herunder tydeliggjøre rutiner for regelmessig revisjon	31.03.2024
2	Utarbeide opplæringsmaterieell (brukerveiledninger og veiledninger) for ny tilgangsstyringsløsning, herunder etablere rutiner som sikrer at alle ledere og identadministratorer får opplæring før de kan håndtere tilgangsstyring	31.12.2024
3	Gjennomgå og oppdatere gjeldende rutiner for tildeling av tilganger i sentrale fagsystemer i forbindelse med innføring av ny tilgangsstyringsløsning	31.12.2024
4	Følge opp de enheter som ikke har dokumentert at de har gjennomført årlig tilgangsrevisjon i 2023	31.01.2024
5	Implementere sentralisert rutine i ny tilgangsstyringsløsning for oppfølging av tilgangsrevisjon, herunder kontroll og analyse	31.06.2024
6	Slutføre avvikling av fagsystemet Arena (etablert i 2000) gjennom programmet P4 Flere i arbeid. Programmet startet i 2021 etter planlegging i 2020. Ytelse løftes gradvis over på ny løsning.	31.12.2027
7	Gjennomgå og eventuelt oppdatere rutiner for risikovurderinger og personvernkonsekvensvurdering for å presisere krav til vurdering ved utforming av tilgangsstyring	31.03.2024
8	Oppdatering av risikovurderinger og tilgangsstyring i sentrale fagsystemer i forbindelse med innføring av ny tilgangsstyringsløsning	31.12.2024
9	Innføre ny tilgangsstyringsløsning for NAVs fagsystemer	31.12.2025
10	Gjennomgå og risikovurdere alle tema og vurdere om journal kan skjules for personer som ikke har dokumenttilgang	31.05.2024
11	Per fagområde: Avklare kriterier for når en aktiv sak kan anses som historisk og dermed skjules for ansatte uten særskilt tilgang	31.12.2024
12	Innføre funksjonalitet for å skjule avsluttede saker i noen fagsystemer	31.12.2024
13	Innføre funksjonalitet for å skjule avsluttede saker i alle fagsystemer som har historiske saker som kan skjules	31.12.2025
14	Utrede konsekvenser av skjerming av brukere som ønsker det	31.12.2024
15	Iverksette manuell proaktiv loggkontroll innenfor et hensiktsmessig og begrenset område	31.03.2024
16	Utarbeide gjennomføringsplan for forbedring av loggkontroll	31.05.2024

Samtidig anfører NAV at saken ikke er godt nok opplyst, jf. forvaltningsloven § 17, og at Datatilsynet derfor ikke har grunnlag for å fatte vedtak om lovbrudd innenfor de kontrollerte områdene.

Slik Datatilsynet forstår dette, er påstanden basert på en forutsetning fra NAVs side om at de varslede vedtakene bygger på en «samlet vurdering av *hele* NAV sin virksomhet på personvern- og informasjonssikkerhetsområdet». Våre kommentarer til disse anførselene (del I, punkt 1.2 og 1.3 i tilsvaret) følger under punkt 7 nedenfor.

Vi har gjort enkelte justeringer i ordlyden i påleggene som følge av NAVs kommentarer i del II. Dette er redegjort for i punkt 11 nedenfor. NAVs øvrige kommentarer til vurderingen av lovbruddene, herunder i punkt 1.1 og 1.2 i del I av tilsvaret, er hensyntatt her.

I punkt 1.5 i tilsvaret har NAV kommentert vurderingen av skyldkravet i forbindelse med det varslede overtredelsesgebyret. NAV mener at det ikke er grunnlag for å konstatere skyldgraden forsett.

Vurderingene våre av NAVs anførsler knyttet til overtredelsesgebyr (del I, punkt 1.4 og 1.5 i tilsvaret) følger under punkt 13.2 og 13.3 nedenfor. NAVs innsigelser har ikke medført endring av overtredelsesgebyrets størrelse.

NAV har fremhevet enkelte setninger i varselet om vedtak som de er uenige i. Vi har markert de aktuelle setningene med fotnoter, for å synliggjøre uenigheten og eventuelle endringer vi har gjort på bakgrunn av NAVs merknader.

4. Vedtak om pålegg

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d, fatter vi følgende vedtak:

1. *NAV pålegges å etablere og gjennomføre en helhetlig og egnet systematikk for organisatoriske tiltak for å sikre og påvise etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2, artikkel 24 nr. 1 og 2 og artikkel 32 nr. 1, 2 og 4, da det stedlige tilsynet har avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. Se punkt 4 og 5 (avvik 1 og 2) i tilsynsrapporten og punkt 11.2 nedenfor.*

Herunder må NAV¹:

- a. *Ferdigstille rutiner for regelmessig revisjon av den styrende dokumentasjonen for tilgangsstyring innen 31. mars 2024, da det stedlige tilsynet avdekket at den eksisterende dokumentasjonen ikke er gjenstand for regelmessig revisjon i henhold til kravene i personvernforordningen artikkel 32 nr. 1 bokstav d. Se punkt 5.2.2 (avvik 3) i tilsynsrapporten og punkt 11.2.1 nedenfor.*
- b. *Etablere rutiner som sikrer at tilgangsstyringen tilpasses risikoen ved behandlingen av personopplysninger i de enkelte fagsystemene, da det stedlige*

¹ Pålegg 1 e fra varsel om vedtak bortfaller, jf. punkt 11.2.5 nedenfor.

tilsynet avdekket at de eksisterende rutinene ikke sikrer at det ved vurderingen av egnet sikkerhetsnivå (tilgangsnivå) tas hensyn til risikoene forbundet med behandlingen, jf. personvernforordningen artikkel 32 nr. 2. Se punkt 5.2.2 (avvik 4) i tilsynsrapporten og punkt 11.2.2 nedenfor.

- c. Ferdigstille rutiner for opplæring av identadministratorer innen 31. desember 2024, da det stedlige tilsynet avdekket at det ikke er etablert tilfredsstillende organisatoriske tiltak for opplæring av denne gruppen, jf. personvernforordningen artikkel 32 nr. 1 og nr. 4. Se punkt 5.3.2 og 5.4.2 (avvik 6) i tilsynsrapporten og punkt 11.2.3 nedenfor.*
 - d. Etablere og ferdigstille oppdaterte og egnede rutiner for tildeling av tilganger i de ulike fagsystemene innen 31. desember 2024, da det stedlige tilsynet avdekket at de eksisterende rutinene er utdaterte og mangelfulle, og således ikke oppfyller kravene i personvernforordningen artikkel 32 nr. 1 og nr. 4. Se punkt 5.4.2 (avvik 7) i tilsynsrapporten og punkt 11.2.4 nedenfor.*
- 2. NAV pålegges å etablere tekniske og organisatoriske tiltak knyttet til tilgangsstyring som gir tilfredsstillende konfidensialitetssikring av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, da det stedlige tilsynet avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. Se punkt 5 (avvik 9) i tilsynsrapporten og punkt 11.3 nedenfor.*

Herunder må NAV:

- a. Innen 31. mai 2024 etablere tekniske og organisatoriske tiltak for arkivsystemet Joark som begrenser tilgang til metadata om dokumenter på tvers av fagområder til tilfeller hvor det er nødvendig, da det stedlige tilsynet avdekket at tilgjengeliggjøringen av slike data er for generell og vid, og således ikke oppfyller kravene i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. Se punkt 5.3.2 (avvik 5) i tilsynsrapporten og punkt 11.3.1 nedenfor.*
- b. Innen 31. desember 2025 etablere tekniske og organisatoriske tiltak for å begrense tilgangen til personopplysninger som kun behandles for arkivformål (historiske saker) til tilfeller hvor det er nødvendig, da det stedlige tilsynet avdekket at tilgangen til historiske saker er for generell og vid, og således ikke oppfyller kravene i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. Se punkt 5.4.2 (avvik 8) i tilsynsrapporten og punkt 11.3.2 nedenfor.*
- c. Etablere tekniske og organisatoriske tiltak som gir mulighet for å tilpasse personopplysningssikkerheten ut fra risiko begrunnet i konkrete brukerbehov, da det stedlige tilsynet avdekket at de eksisterende tiltakene ikke gir en slik mulighet, og følgelig ikke oppfyller kravene til at sikkerhetstiltakene tilpasses risikoen ved behandlingen jf. personvernforordningen artikkel 32 nr. 1. Se punkt 5.7.2 (avvik 10) i tilsynsrapporten og punkt 11.3.3 nedenfor.*

3. NAV pålegges å etablere tekniske og organisatoriske tiltak knyttet til loggkontroll som gir tilfredsstillende konfidensialitetssikring av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1 bokstav d og nr. 4, da det stedlige tilsynet avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. Se punkt 7 (avvik 12) i tilsynsrapporten og punkt 11.4 nedenfor.

5. Frister for gjennomføring

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d, kan Datatilsynet sette frister for gjennomføring av påleggene.

NAV må rapportere kvartalsvis på fremdrift og oppfyllelse av samtlige pålegg, med første rapportering primo juni 2024.

NAV har bestridt de overordnede påleggene i nr. 1 og 2. Det er følgelig ikke lagt noen plan fra NAVs side for å utbedre avvik 1, 2 og 9. Datatilsynet har ikke imøtekommet NAVs innsigelser på disse punktene, og det må utarbeides en plan for gjennomføring av også disse påleggene. Frist for dette settes til første kvartalsrapportering.

Tiltakene NAV har planlagt for å etterkomme pålegg 2 c og 3 oppfyller ikke påleggene fullt ut. For disse påleggene mener NAV at det er nødvendig med en nærmere utredning før de kan binde seg til konkrete tiltak. Datatilsynet har forståelse for dette og vil fastsette konkret frist for oppfyllelse når NAV har gjennomført den planlagte utredningen.

6. Vedtak om ileggelse av overtredelsesgebyr

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, fatter vi følgende vedtak:

NAV ilegges et overtredelsesgebyr på 20 000 000 – tjue millioner – kroner for overtredelse av

- a) *personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4, som følge av behandling av personopplysninger på en måte som ikke sikrer tilstrekkelig sikkerhet for personopplysningene, og*
- b) *personvernforordningen artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2, som følge av ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen.*

7. Tilsynets omfang og sakens opplysning

7.1 Omfang

NAV skriver i sitt tilsvarende at de baserte sin deltakelse under det utførte tilsynet på de tematiske avgrensningene som fremgikk av Datatilsynets varsel om tilsyn av 1. mars 2023, dvs. tilgangsstyring, logg og loggkontroll. NAV oppfatter imidlertid det etterfølgende varselet om vedtak slik at dette baserer seg på «en samlet vurdering av *hele* NAV sin virksomhet på personvern- og informasjonssikkerhetsområdet», og at Datatilsynet således har gått ut over de angitte avgrensningene i sin vurdering av funn fra tilsynet.

Datatilsynet er ikke enig i denne anførselen fra NAV. I varselet om tilsyn av 1. mars 2023 avgrenset vi kontrollen til temaene tilgangsstyring, logg og loggkontroll. Vi varslet også om at vi ville kontrollere «at NAV har etablert et tilfredsstillende styringssystem for personopplysningssikkerhet, knyttet til forvaltningen av autorisasjoner i fagsystemene og evne til å tilpasse sikkerhetsnivået for personer som har et særskilt beskyttelsesbehov». Disse avgrensningene har stått uendret gjennom hele tilsynsprosessen. NAV har ikke stilt spørsmål ved avgrensningen tidligere.

Lovbruddene som er avdekket gjennom tilsynet knytter seg til konkrete mangler som ligger innenfor det varslede tilsynets tematiske avgrensninger. Overtredelsesgebyret er en reaksjon på lovbruddene. Det er ikke riktig at vedtaket er basert på en generell vurdering av alt personvernarbeidet i NAV.

Tilsynet ble påbegynt i mars 2023, og frem mot varsel om vedtak har det vært skriftlig korrespondanse og møter mellom NAV og Datatilsynet. Avgrensningene er gjentatt muntlig i møter med NAV 14. mars 2023, 23. august 2023 og 6. september 2023, og skriftlig i foreløpig tilsynsrapport av 1. november 2023 (punkt 1), endelig tilsynsrapport av 27. november 2023 (punkt 1) og varsel om vedtak 27. november 2023 (punkt 2). NAV ga ikke på noe tidspunkt uttrykk for at Datatilsynet hadde gått utenfor det varslede tilsynstemaet.

Vår oppfatning er at Datatilsynet og NAV har hatt en omforent forståelse av tilsynets omfang gjennom hele tilsynsprosessen. NAV har heller ikke begrunnet hvorfor de ser annerledes på dette nå. Datatilsynet finner etter dette ikke grunnlag for å legge vekt på denne anførselen i den videre behandlingen av tilsvaret fra NAV.

7.2 Opplysning av saken

7.2.1 NAVs anførsler om opplysning av saken

NAV fremholder i punkt 1.2 i tilsvaret at vedtakene som er varslet «ikke er godt nok utredet jf. forvaltningsloven § 17». NAV skriver videre at «Datatilsynet på det grunnlaget som har vært gjenstand for tilsyn ikke har tilstrekkelig dokumentasjon for å fatte vedtak om brudd på artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4, ei heller grunnlag for å konstatere brudd på personvernforordningen artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2».

I punkt 1.3 følger en liste over tiltak NAV har iverksatt de siste årene for å styrke personvernet og sørge for etterlevelse av personvernregelverket. Tiltakene kan til dels anses som elementer i NAVs styringssystem, noe som har vært et tema i tilsynet, men gjelder i hovedsak områder som ikke er relevante for saken (for eksempel «behandlingsoversikt», «organisering av juridiske funksjoner» og «overføring av personopplysninger til tredjeland»). NAV fremholder i sitt tilsvaret at denne listen «må anses som vår begrunnelse for at vedtaket ikke er tilstrekkelig utredet, ikke et forsøk på opplysning og utredning av saken».

7.2.2 Datatilsynets vurdering av NAVs forutsetning om et uavgrenset omfang

NAVs anførsler på dette punktet fremstår som bundet til forutsetningen om at vedtaket er basert på en «samlet vurdering» av personvernarbeidet i NAV. Denne forutsetningen er ikke riktig, jf. punkt 7.1 ovenfor.

Vi viser til at NAV «i stor grad er enig» i lovbruddene. NAV har således bekreftet at faktagrunnlaget for konklusjonene er tilstrekkelig, jf. også punkt 7.2.5 nedenfor.² Dette er gjenspeilet i tiltakene NAV har planlagt for å rette lovbruddene. Vi må derfor kunne legge til grunn at NAV – sett bort fra den uriktige forutsetningen – er enige i at saken er tilstrekkelig opplyst (jf. forvaltningsloven § 17), selv om NAV er uenige i enkelte av konklusjonene våre.

Overtredelsesgebyret er en reaksjon på lovbruddene, og det er beregnet på bakgrunn av en vurdering av lovbruddenes alvorlighetsgrad. Faktagrunnlaget for vedtakene om pålegg (som korresponderer med lovbruddene) og vedtaket om overtredelsesgebyr kan ikke isoleres fra hverandre.

Datatilsynet mener i alle tilfeller at avgjørelsen i saken er riktig.

7.2.3 Rettslig regulering av Datatilsynets utredningsplikt og NAVs opplysningsplikt

Det følger av utredningsplikten i forvaltningsloven § 17 at Datatilsynet «skal påse at saken er så godt opplyst som mulig før vedtak treffes». Datatilsynet skal samtidig legge til rette for at partene i saken gir de relevante opplysningene, jf. veiledningsplikten i forvaltningsloven § 11. Omfanget av veiledningsplikten må tilpasses partene.

Kravene til opplysning av saken etter forvaltningsloven § 17 må sees i sammenheng med NAVs opplysningsplikt, jf. personvernforordningen artikkel 58 nr. 1 bokstav a. Etter denne bestemmelsen plikter NAV «å framlegge all informasjon [Datatilsynet] trenger for å kunne utføre sine oppgaver», når vi gir pålegg om det.

I juridisk teori³ er partenes eget ansvar for å opplyse saken beskrevet slik:

«Selv om de ikke har plikt til det, må forvaltningen kunne regne med at partene i noen grad selv bidrar til sakens opplysning når (...) de oppfordres til det. I det minste må

² Med de modifikasjonene som følger i del II av tilsvaret (se nærmere om dette under punkt 11).

³ Torstein Eckhoff og Eivind Smith, Forvaltningsrett, 12. utgave, Universitetsforlaget, 2022 s. 278, Juridika (kopiert 24. januar 2024) <https://juridika.no/fagbok/forvaltningsrett/12/dokument#ii-utredningsplikten>

man kunne vente at partene opplyser om slike forhold som de må forstå vil styrke deres sak. Som utgangspunkt kan forvaltningen derfor ikke bebreides om opplysninger til gunst for en part, ikke er kommet frem fordi parten har unnlatt å oppfylle sin opplysningsplikt, eller ikke har fulgt oppfordringer om å opplyse om forholdet. Men vurderingen må også ta hensyn til partens forutsetninger for å forstå hva som er relevant».

NAV har altså et selvstendig ansvar for å vurdere hvilke opplysninger som er relevante å fremlegge i saken. Dette innebærer at NAVs opplysningsplikt kan omfatte mer enn den spesifikke informasjonen de blir pålagt å fremlegge. Dersom NAV har annen informasjon som er nødvendig for at Datatilsynet skal kunne ha et forsvarlig avgjørelsesgrunnlag, men som tilsynet selv ikke har forutsetninger til å vite om og etterspørre, plikter NAV å fremlegge denne informasjonen av eget initiativ. Det er videre også opp til NAV å stille med de menneskelige ressursene som har kompetanse til å svare på spørsmål innenfor sakens tema når de er gjenstand for et stedlig tilsyn.

7.2.4 Tilsynsprosessen – Datatilsynets opplysning av saken og veiledning til NAV

NAV ble gitt pålegg om å gi informasjon i vårt varsel om tilsyn av 1. mars 2023, i tråd med personvernforordningen artikkel 58 nr. 1 bokstav a. Spørsmålene vi stilte under tilsynet 6. september 2023 var også å anse som pålegg om å gi informasjon etter denne bestemmelsen. Ved begge anledninger informerte vi NAV om at de hadde adgang til å klage på påleggene om å gi informasjon. NAV benyttet ikke klageadgangen.

I denne saken mener vi at NAV gjennom informasjon i vår skriftlige korrespondanse har hatt svært gode forutsetninger for å forstå hvilken informasjon det var relevant å fremlegge. Dette ble presentert for NAV i tabell-/listeforamt (vedlegg til tilsynsvarselet). NAV hadde seks måneder til å fremskaffe informasjonen.

I tilsynsvarselet tilbød vi NAV et møte for å avklare eventuelle spørsmål de hadde til pålegget om å gi informasjon. Dette møtet ble avholdt 14. mars 2023. I møtet fremstod NAV som innforstått med innholdet i pålegget. NAV ga uttrykk for at det ville bli en stor jobb å samle og strukturere den etterspurte informasjonen om hvert enkelt fagsystem. Av hensyn til omfanget ble den opprinnelige fristen for å oppfylle pålegget om å gi informasjon forlenget fra 20. april 2023 til 1. juni 2023. Det ble også avtalt at NAV kunne systematisere informasjonen slik de fant det mest hensiktsmessig. Det innebar at de ikke var bundet av tabell-/listeforamtet Datatilsynet hadde utarbeidet.

Enkelte detaljer ble videre avklart per e-post 3. april 2023 og i et nytt møte med NAV 14. april 2023. Foranledningen var blant annet at NAV hadde spørsmål til hvordan de skulle angi antall ansatte med tilgang til de ulike fagsystemene.

NAV oversendte informasjon i henhold til pålegget i tilsynsvarselet i separate bolker hhv. 20. april 2023 og 31. mai 2023. Totalt utgjorde dette ca. 70 dokumenter, og inkluderte blant annet dokumentasjon på gjeldende retningslinjer og rutiner innen tilgangsstyring, logging og

loggkontroll, detaljerte opplysninger om hvordan dette er implementert i 55 sentrale fagsystemer, og en forklarende redegjørelse som NAV laget i sakens anledning.

Den 23. august 2023 ble det avholdt et formøte til det stedlige tilsynet, hvor Datatilsynet igjen orienterte om tilsynets omfang og avgrensninger, og presenterte en agenda med angivelser av hvilke tidspunkt ulike tema ville bli behandlet under besøket 6. september 2023. Agendaen ble oversendt NAV etter møtet.

Den 27. august 2023 oversendte NAV to sentrale dokumenter som de da hadde oppdaget at ikke var sendt tidligere (*Styringsdokumentet for sikkerhet og Standard for tilgangsforvaltning*).

Under tilsynet 6. september 2023 ble deltakerne fra NAVs side informert om at spørsmålene våre var å anse som pålegg om å gi informasjon, som kunne påklages, og at de også hadde anledning til å ettersende svar på spørsmål de ikke var i stand til å besvare der og da. De fikk også informasjon om at ettersendte dokumenter ville hensyntas i tilsynsrapporten.

Deltakerne fra NAV svarte på de fleste spørsmålene vi hadde. NAV benyttet også muligheten til å ettersende informasjon. Ytterligere redegjørelser og ti nye dokumenter ble fremlagt 14. september 2023.

7.2.5 NAVs muligheter for kontradiksjon

Faktagrunnlaget for vedtakene er NAVs forhåndsinnsendte dokumentasjon, informasjonen som fremkom under det stedlige tilsynet 6. september 2023 og ettersendt dokumentasjon som ble fremlagt 14. september 2023. Dette er beskrevet i tilsynsrapporten og i varselet om vedtak.

NAV fikk tilsendt den foreløpige tilsynsrapporten 1. november 2023, hvor de ble bedt om «å korrigere eventuelle feil eller ufullstendige opplysninger i vår forståelse av faktum».

I NAVs tilbakemelding 6. november 2023, skriver de:

«Rapporten har i stor grad en presis og korrekt beskrivelse av fakta. Det er noen få faktafeil som vi mener gir et feilaktig bilde av omfang av opplysninger som saksbehandlere får tilgang til. Om mulig så ønsker vi at teksten korrigeres før det gis innsyn i foreløpig tilsynsrapport slik at det ikke skapes et unødvendig negativt bilde av NAVs behandling av personopplysninger.» (Datatilsynets utheving.)

I den utfyllende tilbakemeldingen fra NAV 22. november 2023, viser NAV til «Datatilsynets oversendelse av foreløpig tilsynsrapport av 01.11.2023, der Arbeids- og velferdsdirektoratet gis anledning til å korrigere eventuelle feil eller ufullstendige opplysninger», og skriver videre:

«Det er enkelte fakta som er unøyaktige eller feil, og beskrivelser som vi mener gir et noe feilaktig bilde av omfang av hvordan tilgangsstyring og tilgangskontroll gjennomføres, hvilke opplysninger som saksbehandlere får tilgang til og omfanget av

tilgang. Flere av innspillene sendte vi også 06.11.2023, men vi har nå lagt til ytterligere informasjon.» (Datatilsynets uthevinger.)

Tilleggsinformasjonen NAV ga ved disse to anledningene er i sin helhet tatt inn i den endelige tilsynsrapporten og er tatt høyde for i de varslede vedtakene. Tilføyelsene er markert med fotnoter i den endelige rapporten.

7.2.6 Datatilsynets vurdering av sakens opplysning

På bakgrunn av gjennomgangen over er det etter Datatilsynets oppfatning klart at Datatilsynets utrednings- og veiledningsplikt etter forvaltningsloven §§ 17 og 11 er oppfylt. NAV har fått og benyttet flere anledninger til å fremlegge utfyllende faktaopplysninger, og har fått muntlig og skriftlig informasjon om muligheten til å be om ytterligere veiledning ved behov. Dette har de til dels benyttet seg av, men det har ikke på noe tidspunkt blitt fremholdt at Datatilsynets vurderinger og funn går ut over det oppgitte tilsystemet.

7.2.7 Nye opplysninger 4. januar 2024

I NAVs tilsvarende av 4. januar 2024 er det fremlagt en rekke nye opplysninger. Vi legger til grunn at NAV med dette har oversendt all relevant dokumentasjon.

Vi vil ikke gjøre endringer i den endelige tilsynsrapporten av 27. november 2023. Rapporten gir et situasjonsbilde som NAV har korrigert tidligere, jf. punkt 7.2.5. Nye opplysninger er imidlertid hensyntatt ved vår vurdering av om vedtakene skal fattes i tråd med varselet.

8. Personvern i NAV

NAV er en landsdekkende offentlig virksomhet, og består av både kommunale og statlige tjenester. NAV består av den statlige arbeids- og velferdsetaten og partnerskapet med hver enkelt kommune. NAV har ansvar for å forvalte velferdstjenester som arbeidsmarkedstiltak, trygdeytelser og sosialhjelp.

NAV står i en særstilling sett fra et personvernperspektiv. Oppgavene NAV er pålagt medfører behandling av personopplysninger om nesten alle innbyggere i Norge og i et enormt omfang, herunder svært sensitive opplysninger. Ifølge tall fra NAVs årsrapport for 2022, var det i 2022 ca. 3,2 millioner personer som mottok ytelser fra NAV.

Det ligger derfor en iboende høy personvernrisiko i NAVs virksomhet, som innebærer at det må stilles strenge krav til personopplysningssikkerheten i etaten.

Denne risikoen ble identifisert og påpekt allerede ved vedtakelsen av lov 16. juni 2006 nr. 20 om arbeids- og velferdsforvaltningen (NAV-loven). I høringsrunden uttrykte Datatilsynet bekymring for at reformen ville medføre en vesentlig tilgjengeliggjøring av sensitiv informasjon om den enkelte. Datatilsynets høringsuttalelse er gjengitt slik i forarbeidene til NAV-loven (på side 66 i Ot.prp. nr. 47 (2005-2006)):

«Totalt sett fremstår ikke forslaget, etter Datatilsynets oppfatning, som egnet til å skape tillit til den nye etaten i befolkningen. For Datatilsynet vil det være uakseptabelt dersom en ved sammenslåingen ikke legger til grunn et prinsipp - også for utviklingen av IKT-systemet, om at ingen skal ha tilgang til flere personopplysninger enn de som de trenger for å utøve sine arbeidsoppgaver forsvarlig, og at ethvert oppslag de ansatte gjør skal logges og loggene kontrolleres.»

Arbeids- og inkluderingsdepartementet kommenterte vårt og andre høringsinstansers syn slik på side 71 i proposisjonen:

«Hensynet til taushetsplikt og personvern må ivaretas ved summen av de lovreglene, sikkerhetstiltak, prosess og mekanismer for styring av tilgang til informasjon i IKT-systemene og regimet for kontroll og oppfølging av dette som tilrettelegges. For å ivareta informasjonssikkerhet, herunder sikre prinsippet om at ingen skal ha tilgang til flere personopplysninger enn det de trenger for å utøve sine arbeidsoppgaver, er det viktig med et kontrollregime som følger opp informasjonssikkerheten.

Både etaten og de felles lokale kontorene vil forvalte store mengder sensitive personopplysninger. Dersom det ikke etableres et tydelig regime for informasjonssikkerhet, er dette en risiko.»

Det har med andre ord vært en kjent forutsetning, helt siden opprettelsen av NAV, at ivaretagelse av personopplysningssikkerhet – særlig i form av konfidensialitetssikring – må være en sentral del av virksomheten.

9. Hovedfunn i det stedlige tilsynet

Hovedfunnene i tilsynet er at NAV har organisert seg slik at et stort antall ansatte jobber med saker fra hele landet, innen flere tjenesteområder, og følgelig har tilsvarende vide tilganger. Samtidig er det ikke etablert noen systematisk kontroll av ansattes bruk av fagsystemene. Resultatet av dette er, slik vi ser det, at bruken av fagsystemene i stor grad er tillitsbasert. Manglende rutiner og styring gjør at ansatte ikke har verktøyene de trenger for å forvalte den tilliten og det ansvaret de gis.

Tilsynet avdekket 12 lovbrudd. Vi viser til vurderingene våre, og til beskrivelsene av de faktiske og rettslige forholdene i saken, slik de er omtalt i den endelige tilsynsrapporten. Konklusjonene lyder som følger:

- **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. Se rapporten punkt 4.
- **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 rapporten 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 rapporten 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 rapporten 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 rapporten 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 rapporten punkt 5.3 og 5.4.
- **Avvik 7:** Rutinene for tildeling av tilganger er utdaterte og gir ingen veiledning knyttet til skjønnsmessige vurderinger. Dette er å regne som et avvik fra kravene til organisatoriske tiltak etter personvernforordningen artikkel 32 nr. 1 og nr. 4. Se rapporten 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 rapporten 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 rapporten punkt 7) er dette ikke forenlig med konfidensialitetsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav f og kravene til personopplysningssikkerhet i artikkel 32 nr. 1. Se rapporten 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 rapporten 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 rapporten punkt 5.8.

- **Avvik 12:** NAV har ikke etablert en systematisk loggkontroll. I kombinasjon med at en betydelig andel av NAVs ansatte har vide tilganger (se rapporten 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. Se rapporten punkt 7.

Avvik 11 bortfaller på grunnlag av nye opplysninger fra NAV i tilsvaret av 4. januar 2024. Se punkt 11.2.5.

Vi noterte oss under tilsynet at NAVs sikkerhetsrammeverk er under revidering. NAV har et mål om å slutføre dette arbeidet i 2026. Vi presiserer derfor at vurderingene våre tar utgangspunkt i NAVs praksis og etterlevelse av regelverket på tidspunktet for tilsynet.

Vi vil også presisere at vi utelukkende har sett på den interne personopplysningssikkerheten. Vide tilganger og manglende bruk av logger kan også gjøre NAV sårbare for eksterne sikkerhetstrusler.

10. Tidligere tilsyn og evalueringer mv. av NAV

10.1 Tilsyn i 2007

Datatilsynet kontrollerte personopplysningssikkerheten i NAV gjennom fire tilsyn i 2007 (saksnummer 07/01456, 07/01457, 07/01458 og 07/01459). Tilsynet med saksnummer 07/01456 var rettet mot NAV sentralt, mens de øvrige tilsynene var rettet mot ulike lokalkontor.

Datatilsynet fant avvik knyttet til tilgangsstyring, logging og loggkontroll. Dette resulterte i bl.a. følgende pålegg (sak 07/01456):

1. *«Arbeids- og velferdsdirektoratet må etablere tilfredstillende informasjonssikkerhet hva gjelder tilgangsstyring og logging i samsvar med personopplysningslovens § 13, jf. personopplysningsforskriftens § 2-11. Det vises til kontrollrapportens punkt 8.1.5.1.»*
2. *Arbeids- og velferdsdirektoratet må begrense gitte tilganger ved NAV Lier i samsvar med personopplysningslovens § 13, jf. personopplysningsforskriftens § 2- 11. Det vises til kontrollrapportens punkt 8.1.5.2.»*
3. *Arbeids- og velferdsdirektoratet må avslutte bruken av Arena som et felles oppfølgingsverktøy med mindre det etableres sikkerhetstiltak i samsvar med personopplysningslovens § 13, jf. personopplysningsforskriftens §§ 2-7, 2-8, 2-11 og 2-14. Det vises til kontrollrapportens punkt 8.2.3.»*

Blant hovedfunnene i tilsynsrapporten var at den enkelte medarbeider hadde fått en betydelig større tilgang til personopplysninger gjennom NAV-reformen, og at NAV syntes å ha valgt et

verktøy for å følge opp den enkelte tjenestemottaker uten at det var etablert grunnleggende informasjonssikkerhetstiltak.

10.2 Tilsyn i 2010

Datatilsynet kontrollerte personopplysningssikkerheten i NAV på nytt i 2010 (sak 10/01228). Avvikene knyttet til tilgangsstyring, logging og loggkontroll, som ble konstatert i 2007, var da ikke lukket. Tilsynet resulterte bl.a. i følgende pålegg til NAV:

1. *«Arbeids- og velferdsdirektoratet må etablere logging av oppslag på enkeltpersoner i sine fagsystemer i samsvar med personopplysningslovens § 13, jf. personopplysningsforskriftens §§ 2-8 og 2-14. Det vises til kontrollrapportens punkt 6.4.3.*
2. *Arbeids- og velferdsdirektoratet må etablere tilfredsstillende konfidensialitetssikring hva gjelder tilgangsstyring og bruk av logger i samsvar med personopplysningslovens § 13, jf. personopplysningsforskriftens §§ 2-11 og 2-14. Det vises til kontrollrapportens punkt 6.5.3.»*

10.3 Tilsyn i 2011

I 2011 gjennomførte Datatilsynet et tilsyn (sak 11/00797) med fokus på ansvarsfordelingen mellom den statlige og den kommunale delen av NAV. Datatilsynet kontrollerte samtidig om avvikene som ble konstatert i 2007 og 2010 var lukket.

Fra tilsynsrapportens sammendrag hitsettes:

«Konfidensialitetssikringen i NAV er ikke tilfredsstillende. Dette fordi det gis svært vide tilganger, og logging og bruk av logger er mangelfull. Dette er tidligere dokumentert i kontrollen med direktoratet i 2010. Det er i tillegg ikke etablert tilstrekkelige rutiner for tildeling av tilganger. Manglende konfidensialitetssikring gjelder både kommunale og statlige fagsystem.»

Fra Datatilsynets varsel om pålegg i saken, datert 3. februar 2012, hitsettes:

«Avvik som er dokumentert i foreliggende kontrollrapport bekrefter funn fra tidligere kontroller med Arbeids- og velferdsdirektoratet og tidligere gitt pålegg. Dette gjelder:

1. *Behovet for at arbeids- og velferdsdirektoratet etablerer tilfredsstillende konfidensialitetssikring hva gjelder tilgangsstyring og bruk av logger i samsvar med personopplysningslovens § 13, jf. personopplysningsforskriftens §§ 2-11 og 2-14. Det vises til kontrollrapportens punkt 7.4.6.1.*

Det vises her til Datatilsynets Vedtak om pålegg av 6. mai 2011. Forholdet følges opp i tidligere kontrollsak.»

NAV bekreftet i brev 21. januar 2013 at avvikene var lukket. Datatilsynet la dette til grunn og avsluttet saken 8. februar 2013 uten at det ble fattet noe vedtak i tråd med det varslede pålegget.

10.4 BDO og Wiersholms evaluering av NAV i 2016

Revisjonsselskapet BDO AS og Advokatfirmaet Wiersholm AS utarbeidet en rapport om tilgangskontroller i NAV i 2016, på oppdrag fra NAV.⁴ Deres overordnede vurdering er formulert slik på side 4 i rapporten:

«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.»

10.5 PwCs evaluering av NAV i 2020

I 2020 gjennomførte PwC AS en modenheitsvurdering⁵ av hele Arbeids- og velferdsetaten, med fokus på bl.a. informasjonssikkerhet. Også PwC avdekket en rekke svakheter i sikkerhetsarbeidet hos NAV, særlig knyttet til styringssystemet.

10.6 NOU 2023: 11 – Raskt og riktig

NOU 2023: 11 er en utredning av klage- og ankesystemet i Arbeids- og velferdsetaten og Trygderetten. Utvalget som står bak utredningen konkluderer med at NAVs arbeid med å øke kvaliteten 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.

10.7 Avsluttende merknad – tidligere tilsyns betydning for denne saken

I lys av historikken beskrevet ovenfor anser vi funnene fra det siste tilsynet som meget alvorlige. På områdene tilgangsstyring og loggkontroll vurderer vi dagens tilstand som tilsvarende eller forverret siden tidligere tilsyn.⁶ I vår vurdering av nødvendigheten av å

⁴ *Tilgangskontroller i NAV – Gjennomgang, analyse og forslag til forbedringer* (13.10.2016), BDO og Wiersholm. Tilgjengelig via nettsiden <https://jusboka.no/wp-content/uploads/2016/11/Rapport-om-tilgangskontroller-i-NAV.pdf?x22677>.

⁵ *Modenheitsvurdering sikkerhet* (november 2020), PwC AS. Rapporten er unntatt offentlighet og omtales derfor kun svært kort her.

⁶ NAV skriver i kommentarene av 4. januar 2024: «Vi er ... ikke enige i Datatilsynet sin vurdering om at «På områdene tilgangsstyring og loggkontroll vurderer vi dagens tilstand som tilsvarende eller forverret siden tidligere tilsyn». NAV har de senere år gjennomført en betydelig prioritering av personvern-området, både når det gjelder teknisk utvikling, kompetanse og strukturer».

Datatilsynet fastholder vurderingen, og viser til at NAV i dag har svakere loggkontroll enn tidligere, samtidig som praksisen med landsdekkende tilganger er utvidet. Vi kan ikke se at prioriteringene NAV viser til

ilegge et overtredelsesgebyr i denne saken, har vi sett hen til at tidligere pålegg gitt av Datatilsynet har vist seg ikke å være tilstrekkelig virkningsfulle.

11. Datatilsynets vurdering av NAVs tilsvar og begrunnelse for vedtak om pålegg

11.1 Innledning

Nedenfor følger en oppsummering av NAVs kommentarer til de varslede påleggene, og Datatilsynets vurderinger i lys av deres tilbakemelding.

Som nevnt i punkt 7.2.7, har NAV fremlagt nye opplysninger etter at det ble varslet vedtak i saken. De nye opplysningene vil ikke medføre endringer i den endelige tilsynsrapporten av 27. november 2023. Rapporten gir et situasjonsbilde som NAV har korrigert tidligere. Rapporten må leses i sammenheng med faktabeskrivelsene og vurderingene nedenfor.

11.2 Pålegg 1 – Etablere et helhetlig og egnet styringssystem

Pålegg 1 i varsel om vedtak lyder:

1. *«NAV pålegges å etablere en helhetlig og egnet systematikk for organisatoriske tiltak for å sikre og påvise etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2, artikkel 24 nr. 1 og 2 og artikkel 32 nr. 1, 2 og 4, da det stedlige tilsynet har avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. Se punkt 4 og 5 (avvik 1 og 2) i tilsynsrapporten.*

Herunder må NAV etablere: (...)»

NAV har bestridt at det er «faktisk grunnlag for å pålegge NAV å etablere en helhetlig og egnet systematikk for organisatoriske tiltak for å sikre og påvise etterlevelse av personvernregelverket».

Datatilsynet mener at vurderingen av konkrete områder i et styringssystem må ta utgangspunkt i det overordnede systemet.

Datatilsynet stilte derfor generelle spørsmål om systematikken i NAVs overordnede styringssystem i den innledende delen av tilsynet. Spørsmål knyttet til det generelle styringssystemet har nær relevans for tilsynets øvrige deler, hvor tematikken omhandlet rutiner på mer konkrete områder. De generelle spørsmålene var en nødvendig forutsetning for at Datatilsynet skulle være i stand til å vurdere øvrige tema i tilsynet.

har ført til forbedringer på områdene tilgangsstyring og loggkontroll. Etablering av nye systemer vil ikke alene forbedre situasjonen dersom de grunnleggende problemene videreføres i de nye systemene.

NAV informerte om pågående prosesser for å utbedre generelle og konkrete deler av sitt styringssystem. Datatilsynet stilte også spørsmål om NAVs overordnede styringssystem, ikke kun begrenset til temaene tilgangsstyring, logging og loggkontroll. I denne delen av tilsynet deltok økonomi- og styringsdirektøren i NAV. De faktiske forholdene som kom frem under tilsynet er beskrevet i tilsynsrapporten punkt 4.2.1.

Under behandlingen av temaene tilgangsstyring, logg og loggkontroll spurte vi etter konkrete rutiner, beskrevet i tilsynsrapporten punkt 5-7. Disse etterspurte rutinene er også relevante for den overordnede vurderingen av styringssystemet. I vedtakets varslede pålegg 1 bokstav a-e har Datatilsynet pålagt NAV å etablere rutiner innenfor disse områdene. NAV har i all hovedsak sagt seg enige i at de har mangler sett opp mot regelverkets krav på disse områdene. De manglende organisatoriske tiltakene i form av nødvendige rutiner som er avdekket under tilsynet, underbygger vår vurdering av at styringssystemet ikke er tilstrekkelig egnet.

NAV har i etterkant av deres innspill til den foreløpige kontrollrapporten og mottak av den endelige tilsynsrapporten, sendt nye beskrivelser av sitt styringssystem og rutiner de mener er relevante for tilsynets tema.

De nye beskrivelsene endrer ikke vår vurdering av at styringssystemet har svakheter og mangler i den overordnede systematikken.

Datatilsynet er enige i NAVs beskrivelse av at regelverket legger opp til en viss skjønnsmargin når det gjelder hva som kreves av styringssystemet, ettersom det «skal stå i et rimelig forhold til behandlingsaktivitetene». For NAVs del innebærer dette imidlertid at det stilles strenge krav, ettersom NAV behandler opplysninger om hele Norges befolkning, i alle livsfaser, herunder betydelige mengder opplysninger innenfor det som betegnes som særlige kategorier.

Behovet for et sterkt og velfungerende styringssystem forsterkes ved at de tekniske tiltakene innenfor tilgangsstyring og loggkontroll etter Datatilsynets vurdering er svake.

Basert på NAVs beskrivelser under tilsynet av manglende helhet og systematikk i styringssystemet, understøttet av påviste mangler innenfor konkrete områder, er vår vurdering at det gjeldende styringssystemet ikke er et «[egnet] ... organisatorisk tiltak for å sikre å påvise at deres behandling av personopplysninger utføres i samsvar med personvernforordningen», jf. personvernforordningen artikkel 24 nr. 1 og 2. Vi påpeker at dette er et hovedfunn i PwCs rapport fra 2020.

Sett i sammenheng med de faktiske forholdene som er beskrevet i tilsynsrapportens punkt 4.2.1, mener Datatilsynet at tilsynet har avdekket at dette lovbruddet gjelder systemet generelt og ikke bare de konkrete områdene tilgangsstyring, logg og loggkontroll.

NAV var varslet om at tilsynet ville omhandle deres styringssystem. Uansett har Datatilsynet, med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d) myndighet til å pålegge den behandlingsansvarlige å sørge for at deres behandlingsaktiviteter skjer i samsvar med

bestemmelsene i forordningen, og myndigheten kan ikke anses begrenset av vårt varsel om tilsyn.

Pålegg 1 vedtas etter dette med følgende endringer:

«1. NAV pålegges å etablere og gjennomføre en helhetlig og egnet systematikk for organisatoriske tiltak for å sikre og påvise etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2, artikkel 24 nr. 1 og 2 og artikkel 32 nr. 1, 2 og 4, da det stedlige tilsynet har avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. (...)»

11.2.1 Pålegg 1 a – Revisjon av styrende dokumentasjon

Pålegg 1 a i varsel om vedtak lyder:

- a. *«[NAV må etablere r]utiner for regelmessig revisjon av den styrende dokumentasjonen for tilgangsstyring, da det stedlige tilsynet avdekket at den ikke er gjenstand for regelmessig revisjon i henhold til kravene i personvernforordningen artikkel 32 nr. 1 bokstav d. Se punkt 5.2.2 (avvik 3) i tilsynsrapporten.»*

NAV har lagt følgende plan for å etterkomme pålegget:

Nr.	Tiltak knyttet til pålegg 1 a	Frist
1	Oppdatere den styrende dokumentasjonen for tilgangsstyring, herunder tydeliggjøre rutiner for regelmessig revisjon	31.03.2024

Det fremstår for Datatilsynet som at tiltaket vil oppfylle pålegget. NAV opplyser at arbeidet med å implementere nye rutiner allerede er påstartet. I lys av dette har vi gjort følgende endringer i vedtaket, og pålegg 1a vedtas etter dette med følgende ordlyd:

- a. *«[NAV må f]erdigstille rutiner for regelmessig revisjon av den styrende dokumentasjonen for tilgangsstyring innen 31. mars 2024, da det stedlige tilsynet avdekket at den eksisterende dokumentasjonen ikke er gjenstand for regelmessig revisjon i henhold til kravene i personvernforordningen artikkel 32 nr. 1 bokstav d. (...)»*

11.2.2 Pålegg 1 b - Rutine for gjennomføring av risikovurderinger ved etablering og utvikling av fagsystemer

Pålegg 1 b i varsel om vedtak lyder:

- b. *«[NAV må etablere r]utine for gjennomføring av risikovurderinger ved etablering og utvikling av fagsystemer, da det stedlige tilsynet avdekket at de eksisterende rutinene ikke sikrer at risikovurderinger gjennomføres i henhold*

til personvernforordningen artikkel 32 nr. 2. Se punkt 5.2.2 (avvik 4) i tilsynsrapporten.»

NAV mener at vurderingen som ligger til grunn for pålegg 1 b er feil, og viser til punkt 1.3 i sitt tilsvar, hvor eksisterende rutiner er beskrevet. NAV mener at rutine for risikovurderinger ved etablering og utvikling av fagsystemer ikke var tema under tilsynet.

Av relevans for pålegg 1 b, skriver NAV i tilsvaret punkt 1.3 (side 5):

- «*Etterlevelsesverktøyet*: NAV har utviklet en egen løsning (kjent som etterlevelsesløsning) for å vurdere og dokumentere etterlevelse av lovkrav i NAV, herunder knyttet til behandling av personopplysninger. Løsningen skal brukes av ansatte før en ny behandling av personopplysninger starter. Dette gjelder for alle typer behandlinger, herunder i oppgaver knyttet til saksbehandling, utvikling og digitalisering av eksisterende og nye løsninger, anskaffelse av nye systemer og verktøy mv. Etterlevelsesløsning tvinger ansatte til å forholde seg til og ta stilling til personvernkrav. Løsningen inneholder også suksesskriterier og relevant veiledning for å støtte ansatte i deres arbeid.»
- «*TryggNOK – ROS*: For å dokumentere risiko og tiltak knyttet til informasjonssikkerhet har NAV en egenutviklet løsning for gjennomføring, dokumentasjon av risiko, sannsynlighet/ konsekvens og tiltak knyttet til operative risiko- og sårbarhetsanalyser (ROS)».

Når det gjelder risikovurderinger knyttet til tilgangsstyring, viser NAV til tiltakene som er planlagt for å etterkomme pålegg 1 d og 2:

Nr.	Tiltak knyttet til pålegg 1 d	Frist
3	Gjennomgå og oppdatere gjeldende rutiner for tildeling av tilganger i sentrale fagsystemer i forbindelse med innføring av ny tilgangsstyringsløsning	31.12.2024

Nr.	Tiltak knyttet til pålegg 2	Frist
6	Slutføre avvikling av fagsystemet Arena (etablert i 2000) gjennom programmet P4 Flere i arbeid. Programmet startet i 2021 etter planlegging i 2020. Ytelse løftes gradvis over på ny løsning.	31.12.2027
7	Gjennomgå og eventuelt oppdatere rutiner for risikovurderinger og personvernkonsekvensvurdering for å presisere krav til vurdering ved utforming av tilgangsstyring	31.03.2024
8	Oppdatering av risikovurderinger og tilgangsstyring i sentrale fagsystemer i forbindelse med innføring av ny tilgangsstyringsløsning	31.12.2024
9	Innføre ny tilgangsstyringsløsning for NAVs fagsystemer	31.12.2025

Datatilsynet vil først bemerke at vi ser at det varslede pålegg 1 b var upresist formulert fra vår side, og at innholdet i pålegget er vanskelig tilgjengelig for andre enn dem som var tilstede under tilsynet. Dette kan ha påvirket NAVs tilbakemelding.

Kravene til personopplysningssikkerhet etter personvernforordningen artikkel 32 nr. 1 innebærer at tiltakene skal resultere i et sikkerhetsnivå som er «egnet med hensyn til risikoen». Dette forutsetter at den behandlingsansvarlige gjennomfører risikokartlegging og risikovurderinger, og at identifisert risiko hensyntas ved utformingen av sikkerhetstiltakene, hvilket er uttrykkelig påkrevd i artikkel 32 nr. 2.

Tilgangsstyring er et sikkerhetstiltak, og det skal ligge en risikovurdering til grunn for fastsettingen av egnet tilgangsnivå. Risikovurderinger faller derfor klart innenfor tilsynets tematiske avgrensning. Dette ble også belyst under tilsynet, se nederst på side 11 flg. i tilsynsrapporten. Konteksten her var tilgangsstyring som sikkerhetstiltak. Datatilsynet spurte NAV om hvordan de sikrer at tilgangsstyringen tilpasses risikoen ved behandlingen av personopplysninger i de enkelte fagsystemene.

Basert på NAVs svar under tilsynet og dokumentasjonen som ble forhånds- og ettersendt, er vår oppfatning at det ikke gjøres rutinemessige vurderinger av risiko, herunder knyttet til å tilgjengeliggjøre personopplysninger for ansatte (med unntak av opplysninger knyttet til personer som lever på det som kalles kode 6 og 7), før tilgangsnivået i et fagsystem fastsettes. Det fremstår derfor som at det ikke rutinemessig gjøres nødvendige «koblinger» mellom risikonivå og tilgangsnivå. Meningen med pålegg 1 b er at NAV må etablere slike koblinger. Vi ser at dette beklageligvis ikke fremgikk tydelig nok i påleggets opprinnelige formulering.

Beskrivelsene av «Etterlevelsesverktøyet» og «TryggNOK» i tilsvaret punkt 1.3 er generelle. NAV har ikke beskrevet om eller hvordan risikovurderingene som utarbeides gjennom disse løsningene påvirker tilgjengeliggjøringen av personopplysninger i fagsystemene. Tiltak nr. 3 og 6-9 (særlig tiltak nr. 7) kan gi inntrykk av at det foreligger spesifikke rutiner for dette. NAV har imidlertid ikke fremlagt disse rutinene.

Vår vurdering er etter dette at NAV verken har beskrevet eller dokumentert at det foreligger rutiner som svarer ut pålegg 1 b. Vedtaket blir stående frem til NAV eventuelt oversender eksisterende og dekkende rutiner.

For å tydeliggjøre pålegget, har vi gjort endringer i vedtaket. Pålegg 1 b vedtas etter dette med følgende ordlyd:

- b. *«[NAV må etablere rutiner som sikrer at tilgangsstyringen tilpasses risikoen ved behandlingen av personopplysninger i de enkelte fagsystemene, da det stedlige tilsynet avdekket at de eksisterende rutinene ikke sikrer at det ved vurderingen av egnet sikkerhetsnivå (tilgangsnivå) tas hensyn til risikoene forbundet med behandlingen, jf. personvernforordningen artikkel 32 nr. 2. (...)]»*

11.2.3 Pålegg 1 c - Rutine for opplæring av identadministratorer

Pålegg 1 c i varsel om vedtak lyder:

- c. «[NAV må etablere r]utine for opplæring av identadministratorer, da det stedlige tilsynet avdekket at det ikke er etablert tilfredsstillende organisatoriske tiltak for opplæring av denne gruppen, jf. personvernforordningen artikkel 32 nr. 1. og nr. 4. Se punkt 5.3.2 og 5.4.2 (avvik 6) i tilsynsrapporten.»

NAV skriver i sin tilbakemelding at de ser behovet for å forbedre opplæringen av identadministratorer. Samtidig mener de at rapporten ikke gir et riktig bilde av situasjonen, og har fremlagt følgende utfyllende informasjon om rutinene på området:

«Det er etablert beskrivelser av ansvarsområdene og oppgaver til identansvarlige og identadministratorer på Navet (intranett), i tillegg til opplæringsfilmer. Disse opplæringsfilmene erstatter tidligere fysiske kurs (jf. informasjon om dette på intranett). Det er oppgitt kontaktpersoner på nettsiden som kan besvare spørsmål. Det gjennomføres opplæring av nye identadministratorer lokalt, og identadministratorene har digitale møteplasser der de kan stille spørsmål til hverandre og drøfte ulike problemstillinger. Det er i tillegg enkelte veiledninger knyttet til tildeling av enkelttilganger i dagens tilgangsstyringsløsning, i listen «Nytt på Identrutinen» og det er utarbeidet lokale veiledninger.»

NAV har lagt følgende plan for å etterkomme pålegget:

Nr.	Tiltak knyttet til pålegg 1 c	Frist
2	Utarbeide opplæringsmateriell (brukerveiledninger og veiledninger) for ny tilgangsstyringsløsning, herunder etablere rutiner som sikrer at alle ledere og identadministratorer får opplæring før de kan håndtere tilgangsstyring	31.12.2024

Datatilsynet tar de nye opplysningene til etterretning. Vi legger til grunn at det planlagte tiltaket vil avhjelpe de sentrale svakhetene som ble belyst under tilsynet (se særlig side 14 i rapporten), dvs. at opplæring av nye identadministratorer er personavhengig, og at eksisterende rutiner kun beskriver hvordan, men ikke på hvilke vilkår ulike tilganger skal gis.

I lys av NAVs tilbakemelding har vi gjort endringer i vedtaket. Pålegg 1 c vedtas etter dette med følgende ordlyd:

- c. «[NAV må f]lerdigstille rutiner for opplæring av identadministratorer innen 31. desember 2024, da det stedlige tilsynet avdekket at det ikke er etablert tilfredsstillende organisatoriske tiltak for opplæring av denne gruppen, jf. personvernforordningen artikkel 32 nr. 1. og nr. 4. (...).»

11.2.4 Pålegg 1 d - Oppdaterte og egnede rutiner for tildeling av tilganger i de ulike fagsystemene

Pålegg 1 d i varsel om vedtak lyder:

- d. «[NAV må etablere o]ppdaterte og egnede rutiner for tildeling av tilganger i de ulike fagsystemene, da det stedlige tilsynet avdekket at de eksisterende

rutinene er utdaterte og mangelfulle, og således ikke oppfyller kravene i personvernforordningen artikkel 32 nr. 1 og nr. 4. Se punkt 5.4.2 (avvik 7) i tilsynsrapporten.»

I kommentarene til pålegget opplyser NAV at dette er et påstartet arbeid. I den nye tilgangsstyringsløsningen skal rutinene integreres i selve løsningen. Det vil gjøre løsningen mer brukervennlig og effektiv.

NAV har planlagt følgende tiltak for å etterkomme pålegget:

Nr.	Tiltak knyttet til pålegg 1 d	Frist
3	Gjennomgå og oppdatere gjeldende rutiner for tildeling av tilganger i sentrale fagsystemer i forbindelse med innføring av ny tilgangsstyringsløsning	31.12.2024

Det fremstår for Datatilsynet som at tiltaket vil oppfylle pålegget. I vedtaket har vi satt en oppfyllelsesfrist i tråd med NAVs plan:

- d. «[NAV må e]tablere og ferdigstille oppdaterte og egnede rutiner for tildeling av tilganger i de ulike fagsystemene innen 31. desember 2024, da det stedlige tilsynet avdekket at de eksisterende rutinene er utdaterte og mangelfulle, og således ikke oppfyller kravene i personvernforordningen artikkel 32 nr. 1 og nr. 4. (...).»*

11.2.5 Pålegg 1 e - Rutine for kontroll av enhetslederens årlige revisjon av tilganger

Pålegg 1 e i varsel om vedtak lyder:

- e. «[NAV må etablere r]utine for kontroll av enhetslederens årlige revisjon av tilganger, da det stedlige tilsynet avdekket at de eksisterende rutinene ikke oppfyller kravene i personvernforordningen artikkel 32 nr. 1 bokstav d. Se punkt 5.8.2 (avvik 11) i tilsynsrapporten.»*

I kommentarene til det varslede pålegget opplyser NAV at det allerede eksisterer en rutinemessig kontroll av at enhetsledere gjennomfører den årlige revisjonen av tilgangene ved enheten. NAV beskriver dette slik: «Sikkerhetsseksjonen henter i tredje tertial hvert år inn egenerklæringsskjema (digitalt) til avdelinger med linjeansvar der de ber om bekreftelse på at den årlige kontrollen er gjennomført.»

NAV har imidlertid identifisert manglende oppfølging av enhetene som ikke har levert egenerklæringsskjemaet. NAV har lagt en plan for å følge opp de aktuelle enhetene innen 31. januar 2024, samt å implementere en tilsvarende kontrollrutine i den nye tilgangsstyringsløsningen:

Nr.	Tiltak knyttet til pålegg 1 e	Frist
4	Følge opp de enheter som ikke har dokumentert at de har gjennomført årlig tilgangsrevisjon i 2023	31.01.2024

5	Implementere sentralisert rutine i ny tilgangsstyringsløsning for oppfølging av tilgangsrevisjon, herunder kontroll og analyse	31.06.2024
---	--	------------

Vi tar de nye opplysningene til etterretning og legger til grunn at NAV gjennomfører de planlagte tiltakene. Det varslede pålegget anses som oppfylt gjennom rutinen som NAV har beskrevet i kommentarene til varselet. Pålegg 1 e (avvik 11) bortfaller etter dette.

11.3 Pålegg 2 – Tilgangsstyring

Pålegg 2 i varsel om vedtak lyder:

«NAV pålegges å etablere tekniske og organisatoriske tiltak knyttet til tilgangsstyring som gir tilfredsstillende konfidensialitetssikring av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, da det stedlige tilsynet avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. Se punkt 5 (avvik 9) i tilsynsrapporten.

Herunder må NAV etablere: (...)»

NAV skriver i sin tilbakemelding at de mener det i dag er etablert tekniske og organisatoriske tiltak innen tilgangsstyringsområdet som balanserer behovet for likebehandling, kvalitet og effektivitet opp mot konfidensialitet for den registrerte. Dette er utdypet slik:

«Det tjenstlige behovet for tilgang på personopplysninger er sammensatt. Veiledning og informasjon er sentralt i brukernes kontakt med NAV. For at ansatte skal kunne gi veiledning knyttet til brukernes helhetlige behov og samtidig sikre effektivitet ved at bruker får behandlet sin sak innen rimelig tid, må tilgangsstyringen vurderes i et helhetlig perspektiv. Dersom vi hadde organisert NAVs virksomhet med mål om at de ansatte skal ha tilgang til så lite informasjon som mulig om brukerne, ville det mest sannsynlig brutt med både kravet til god veiledning av brukerens helhetlige behov, likebehandling og saksbehandling innen rimelig tid.»

De samme synspunktene kommer til uttrykk i punkt 1.1 i tilsvaret, hvor NAV legger til: «Disse perspektivene er det viktig at vurderingen av eventuelle lovbrudd baserer seg på.»

Videre forklarer NAV at det pågår et arbeid med å implementere en ny teknisk løsning for tilgangsstyring:

«Det ble i 2021 igangsatt et omfattende arbeid med å bytte ut dagens tilgangsstyringsløsning, med en ny løsning som vil bidra til å styrke styringen og kontrollen av tilganger i NAV. Ny teknisk løsning er installert høsten 2023, og fagsystemene vil suksessivt bli koblet på ny løsning i 2024 og 2025. I forbindelse med innføringen av ny løsning vil alle krav, prosesser og risiko gjennomgås og oppdateres, samt at løsningen vil kunne bidra til økt grad av rapportering og mulighet for oppfølging på tilgangsstyringsområdet.»

Med utgangspunkt i dette har NAV utarbeidet en plan som består av følgende fire tiltak:

Nr.	Tiltak knyttet til pålegg 2	Frist
6	Slutføre avvikling av fagsystemet Arena (etablert i 2000) gjennom programmet P4 Flere i arbeid. Programmet startet i 2021 etter planlegging i 2020. Ytelser løftes gradvis over på ny løsning.	31.12.2027
7	Gjennomgå og eventuelt oppdatere rutiner for risikovurderinger og personvernkonsekvensvurdering for å presisere krav til vurdering ved utforming av tilgangsstyring	31.03.2024
8	Oppdatering av risikovurderinger og tilgangsstyring i sentrale fagsystemer i forbindelse med innføring av ny tilgangsstyringsløsning	31.12.2024
9	Innføre ny tilgangsstyringsløsning for NAVs fagsystemer	31.12.2025

Selv om NAV har utarbeidet en tiltaksplan, forstår Datatilsynet tilbakemeldingen slik at NAV mener at de eksisterende tiltakene knyttet til tilgangsstyring gir tilfredsstillende konfidensialitetssikring av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. NAV uttrykker bekymring for at en ordning hvor ansatte har tilgang til «så lite informasjon som mulig» vil medføre at de ikke er i stand til å levere god veiledning og likebehandling, eller å behandle saker innen rimelig tid.

Datatilsynet har forståelse for at hensynet til effektiv saksbehandling er svært viktig i NAVs virksomhet, og at det er et visst behov for generaliserte «nedslagsfelt» i ansattes tilganger. Vi mener samtidig at dette hensynet i for stor grad har gått på bekostning av kravene i personvernregelverket.

Vi mener at NAV presenterer problemstillingen på en unyansert måte. NAV må tilstrebe å finne mer balanserte alternativer enn landsdekkende tilganger på den ene siden, og «så lite informasjon som mulig» på den andre.

En tilgangsstyringsløsning som resulterer i at ansatte som standard har tilgang til opplysninger om hele befolkningen er ikke i tråd med konfidensialitets- og dataminimeringsprinsippene og gir ikke et sikkerhetsnivå som er «egnet med hensyn til risikoen», jf. artikkel 32 nr. 1. Vi kan heller ikke se at NAV har begrunnet at dette, ut fra et effektivitetshensyn, må være løsningen.

Datatilsynet fastholder at det må være mulig for NAV å utøve sine forvaltningsoppgaver godt og effektivt med tilganger som har et snevrere «nedslagsfelt» enn hele landet. NAV vil med enkle midler kunne begrense «reservetilgangene» for den enkelte ansatte betydelig. Som vi har påpekt i tilsynsrapporten, kan det ligge et ubrukt potensial i den eksisterende køordningen hos NAV.

Datatilsynet stiller oss til rådighet for å diskutere alternative muligheter for å komme fram til et resultat som både hensyntar effektivitet i saksbehandlingen og personvernforordningens

krav til å ivareta de registrertes personvern gjennom tekniske og organisatoriske sikkerhetstiltak.

Pålegg 2 vedtas uten endringer.

Vi minner om at pålegget må ses i sammenheng med pålegg 3 (avvik 12) om loggkontroll, ettersom kravene til tilgangsstyring og loggkontroll kan påvirke hverandre.

11.3.1 Pålegg 2 a – Begrensning av tilgang til metadata i Joark

Pålegg 2 a i varsel om vedtak lyder:

- a. *«[NAV må etablere t]ekniske og organisatoriske tiltak for arkivsystemet Joark som begrenser tilgang til metadata om dokumenter på tvers av fagområder til tilfeller hvor det er nødvendig, da det stedlige tilsynet avdekket at tilgjengeliggjøringen av slike data er for generell og vid, og således ikke oppfyller kravene i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. Se punkt 5.3.2 (avvik 5) i tilsynsrapporten.»*

NAV påpeker i sitt tilsvaret at mange fagsystemer kun viser journalposter (metadata) og dokumenter for eget fagområde og for andre fagområder som er direkte relevante for saksbehandlingen. I løsninger for samhandling og oppgaveløsning på tvers (Gosys og Modia Personoversikt) vises metadata på alle områder unntatt FAR (farskap) og KTA (kontroll anmeldelse). Bakgrunnen for dette er at NAV har hatt utfordringer med at informasjon og dokumenter ikke blir gjenfunnet. Det er et sentralt prinsipp i offentlig sektor at borgerne bare skal oppgi informasjon én gang. Det er derfor viktig at NAV er i stand til å gjenfinne informasjon de allerede har.

NAV har lagt en plan for å gjennomgå og vurdere risiko innenfor alle tema, og vurdere om journaldata kan skjules for personer som ikke har dokumenttilgang, innen 31. mai 2024:

Nr.	Tiltak knyttet til pålegg 2 a	Frist
10	Gjennomgå og risikovurdere alle tema og vurdere om journal kan skjules for personer som ikke har dokumenttilgang	31.05.2024

Det fremstår for Datatilsynet som at tiltaket vil oppfylle pålegget. Tiltaket må imidlertid også inneholde gjennomføring av praktisk implementering. I vedtaket har vi satt en oppfyllelsesfrist i tråd med NAVs plan:

- a. *«[NAV må i]nnen 31. mai 2024 etablere tekniske og organisatoriske tiltak for arkivsystemet Joark som begrenser tilgang til metadata om dokumenter på tvers av fagområder til tilfeller hvor det er nødvendig, da det stedlige tilsynet avdekket at tilgjengeliggjøringen av slike data er for generell og vid, og således ikke oppfyller kravene i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. (...)*»

11.3.2 Pålegg 2 b – Begrensning av tilgang til historiske saker

Pålegg 2 b i varsel om vedtak lyder:

- b. «[NAV må etablere t]ekniske og organisatoriske tiltak for å begrense tilgangen til personopplysninger som kun behandles for arkivformål (historiske saker) til tilfeller hvor det er nødvendig, da det stedlige tilsynet avdekket at tilgangen til historiske saker er for generell og vid, og således ikke oppfyller kravene i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. Se punkt 5.4.2 (avvik 8) i tilsynsrapporten.»

NAV er enige i at det er behov for å begrense tilgangen til personopplysninger som kun behandles for arkivformål. Det er ikke nødvendig at alle ansatte som har tilgang til tema og bruker har tilgang til dokumentasjonen fram til dokumentene avleveres til Arkivverket.

NAV beskriver at dette arbeidet vil være omfattende og krevende. Blant annet vil det være krevende å fastsette et skjæringspunkt for når en sak kan anses som historisk.

NAV har utarbeidet en trinnvis tiltaksplan for å etterkomme pålegget. Innen 31. desember 2024 skal kriteriene for når en aktiv sak kan anses som historisk være avklart. Da skal det også være innført funksjonalitet i noen fagsystemer for å skjule historiske saker. Innen 31. desember 2025 skal slik funksjonalitet være innført i alle aktuelle fagsystemer:

Nr.	Tiltak knyttet til pålegg 2 b	Frist
11	Per fagområde: Avklare kriterier for når en aktiv sak kan anses som historisk og dermed skjules for ansatte uten særskilt tilgang	31.12.2024
12	Innføre funksjonalitet for å skjule avsluttede saker i noen fagsystemer	31.12.2024
13	Innføre funksjonalitet for å skjule avsluttede saker i alle fagsystemer som har historiske saker som kan skjules	31.12.2025

Datatilsynet har forståelse for at det vil være tidkrevende å gjennomføre disse prosessene. I vedtaket har vi satt en oppfyllelsesfrist i tråd med NAVs plan:

- b. «[NAV må i]nnen 31. desember 2025 etablere tekniske og organisatoriske tiltak for å begrense tilgangen til personopplysninger som kun behandles for arkivformål (historiske saker) til tilfeller hvor det er nødvendig, da det stedlige tilsynet avdekket at tilgangen til historiske saker er for generell og vid, og således ikke oppfyller kravene i personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1. (...)»

11.3.3 Pålegg 2 c – Mulighet for tilpasning ved særskilt behov for konfidensialitetsvern

Pålegg 2 c i varsel om vedtak lyder:

- c. «[NAV må etablere t]ekniske og organisatoriske tiltak som gir mulighet for å tilpasse personopplysningsikkerheten ut fra risiko begrunnet i konkrete brukerbehov, da det stedlige tilsynet avdekket at de eksisterende tiltakene ikke gir en slik mulighet, og følgelig ikke oppfyller kravene til at sikkerhetstiltakene tilpasses risikoen ved behandlingen jf. personvernforordningen artikkel 32 nr. 1. Se punkt 5.7.2 (avvik 10) i tilsynsrapporten.»

Vi oppfatter at NAV aksepterer pålegget fullt ut. Samtidig skriver NAV at det er behov for å kartlegge alternative løsninger og utrede konsekvenser før de kan forplikte seg til konkrete tiltak. NAV har lagt en plan for å gjennomføre en slik utredning innen 31. desember 2024:

Nr.	Tiltak knyttet til pålegg 2 c	Frist
14	Utrede konsekvenser av skjerming av brukere som ønsker det	31.12.2024

Pålegget vedtas etter dette uten endringer. Oppfyllelsesfristen vil bli fastsatt på et senere tidspunkt, jf. punkt 5. Datatilsynet vil følge opp dette etter at NAV har gjennomført den planlagte utredningen.

11.4 Pålegg 3 – Logg og loggkontroll

Pålegg 3 i varsel om vedtak lyder:

3. «NAV pålegges å etablere tekniske og organisatoriske tiltak knyttet til loggkontroll som gir tilfredsstillende konfidensialitetssikring av personopplysninger, jf. personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1 bokstav d og nr. 4, da det stedlige tilsynet avdekket at de eksisterende tiltakene ikke oppfyller lovens krav. Se punkt 7 (avvik 12) i tilsynsrapporten.»

Vi oppfatter at NAV aksepterer pålegget fullt ut. NAV skriver at det er

«klart for oss at reaktiv loggkontroll ikke er tilstrekkelig, spesielt i kombinasjon med vide tilganger. Vi vil derfor gjøre tiltak både for å forbedre loggkontrollen samtidig som vi også jobber med å gjøre de ansattes tilganger mer presise.

(...)

I perioden august til desember i 2022 gjorde NAV en vurdering av dagens loggløsning inklusive regimet for loggkontroll. Konklusjonen var at det var behov for kortsiktige tiltak i dagens løsning, samt større og mer langsiktige tiltak for å endre eller erstatte dagens loggløsning. I tillegg konkluderte NAV med at det er ønskelig å innføre maskinell proaktiv loggkontroll som et supplement til det eksisterende kontrollregimet.»

Basert på dette har NAV lagt en plan for å gjennomføre følgende tiltak for å etterkomme pålegget:

Nr.	Tiltak knyttet til pålegg 3	Frist
-----	-----------------------------	-------

15	Iverksette manuell proaktiv loggkontroll innenfor et hensiktsmessig og begrenset område	31.03.2024
16	Utarbeide gjennomføringsplan for forbedring av loggkontroll	31.05.2024

Datatilsynet påpeker at pålegget omfatter praktisk implementering av egnede tiltak. Vi vedtar pålegget uten endringer, slik at oppfyllelsesfristen fastsettes på et senere tidspunkt, jf. punkt 5.

Vi bemerker også at tiltakene knyttet til pålegg 2 kan ha innvirkning på hva som anses som egnede tiltak for loggkontroll.

12. Innledende om overtredelsesgebyr

12.1 NAVs kommentarer til varsel om overtredelsesgebyr

NAV stiller spørsmål ved at ingen av de 12 avvikene fra tilsynsrapporten konsumeres av hverandre, ettersom avvikene gjelder samme tematikk og er nært beslektet. NAV viser til EDPBs *Guidelines 04/2022* kapittel 3 og 4 om utmåling av overtredelsesgebyr. Datatilsynets vurdering av dette spørsmålet følger under punkt 13.2.

NAV mener at de ikke har utvist forsett ved overtredelsene. NAV er enige i at overtredelsesgebyr kan ilegges på bakgrunn av anonyme og kumulative feil ved skyldgraden uaktsomhet, men bestrider at det samme er tilfellet ved skyldgraden forsett. NAV bemerker at skylden må referere seg til de nærmere faktiske forholdene som utgjør hvert enkelt lovbrudd. Datatilsynet har vurdert skyldkravet på nytt i lys av NAVs kommentarer, se punkt 13.3.

12.2 Generelt om overtredelsesgebyr

I henhold til personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 andre ledd, kan Datatilsynet ilegge offentlige myndigheter overtredelsesgebyr i tråd med reglene i forordningen artikkel 83 ved brudd på regelverket.

Det er kun overtredelser av bestemmelsene som er oppregnet i artikkel 83 nr. 4 og 5 som kan sanksjoneres med overtredelsesgebyr.

Overtredelsesgebyr er å anse som straff i henhold til Den europeiske menneskerettskonvensjonen artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Det følger av forordningen artikkel 83 nr. 1 at hver tilsynsmyndighet skal sørge for at ilegging av overtredelsesgebyr i hvert enkelt tilfelle er «virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende».

I fortalepunkt 148 er dette utdypet:

«For å styrke håndhevingen av bestemmelsene i denne forordning bør det ved overtredelse av denne forordning ilegges sanksjoner, herunder overtredelsesgebyr, i tillegg til eller i stedet for egnede tiltak som tilsynsmyndigheten pålegger i henhold til denne forordning.»

Vilkårene for ileggelse av gebyr fremgår av forordningen artikkel 83. Bestemmelsen gir i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal tillegges særlig vekt, jf. artikkel 83 nr. 2 bokstav a til k.

EU-domstolen presiserte i sin avgjørelse av 5. desember 2023 i sak C-807/21 (*Deutsche Wohnen*) at vilkårene for ileggelse av overtredelsesgebyr er uttømmende regulert i artikkel 83 nr. 1 til 6. Medlemsstatene har ikke anledning til å fastsette nasjonale tilleggsvilkår. Ut fra dette konkluderte domstolen med at vilkåret i tysk rett om at overtredelsen er begått av en identifisert fysisk person er i strid med personvernforordningen, ettersom et slikt krav ikke kan utledes av forordningen. Domstolen kom til at artikkel 83 skal forstås slik at ileggelse av overtredelsesgebyr er betinget av at den behandlingsansvarlige har utvist skyld i form av uaktsomhet eller forsett.⁷

Når det gjelder gebyrets størrelse, angir artikkel 83 nr. 4 og 5 maksimumssatser avhengig av hvilke bestemmelser i forordningen som er overtrådt. De samme momentene som ved vurdering av om gebyr skal ilegges, skal tillegges særlig vekt også ved utmålingen. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken, samtidig som gebyrets størrelse må stå i et rimelig forhold til overtredelsen og virksomheten, jf. artikkel 83 nr. 1.

13. Vurdering av om overtredelsesgebyr skal ilegges

13.1 Lovkravet

Datatilsynet har kommet til at NAV har brutt personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4. I tillegg har vi kommet til at artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2 er brutt.

Artikkel 24 er ikke nevnt i oppregningen i artikkel 83 nr. 4 og 5. Brudd på denne bestemmelsen kan derfor bare sanksjoneres med overtredelsesgebyr dersom det er bestemt i nasjonal rett. For artikkel 24 er det gitt en slik hjemmel i personopplysningsloven § 26 første ledd, jf. personvernforordningen artikkel 84. Personopplysningsloven § 26 er ikke å regne som et tilleggsvilkår som behandlet i EU-domstolens avgjørelse datert 5. desember 2023 i sak C-807/21 (*Deutsche Wohnen*).

Det foreligger dermed flere lovbrudd som kan gi grunnlag for ileggelse av overtredelsesgebyr, jf. artikkel 83 nr. 4 og 5.

⁷ Jf. også EU-domstolens avgjørelse av 5. desember 2023 i sak C-683/21. Dommene konstaterer Datatilsynets praksis. Dommene innebærer at skyldkravet (uaktsomhet), som Datatilsynet tidligere har utledet av forvaltningsloven § 46, må utledes direkte av personvernforordningen artikkel 83.

13.2 Konkurrence

NAV har stilt spørsmål ved at ingen av de 12 avvikene konsumeres av hverandre, ettersom avvikene gjelder samme tematikk og er nært beslektet.

Datatilsynet har varslet ett samlet gebyr for overtredelse av

- a) personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4, som følge av behandling av personopplysninger på en måte som ikke sikrer tilstrekkelig sikkerhet for personopplysningene, og
- b) personvernforordningen artikkel 5 nr. 2 og artikkel 24 nr. 1 og 2, som følge av ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen.

Grunnlaget for dette er de 12 avvikene som fremgår av tilsynsrapporten, gjengitt i punkt 9 ovenfor. Ett av avvikene anses bortfalt, jf. punkt 11.2.5 ovenfor.

Avvikene anses som selvstendige lovbrudd som på forskjellige måter har innvirkning på konfidensialitetssikringen av personopplysninger i NAV. Datatilsynet har imidlertid tatt hensyn til spørsmålet NAV reiser, ved at ileggelsen av overtredelsesgebyr er basert på en samlet vurdering av alle de selvstendige avvikene.

I vedtaket om pålegg går det frem at Datatilsynet har delt lovbruddene i tre overordnede kategorier, dvs. styringssystem (pålegg 1), tilgangsstyring (pålegg 2) og loggkontroll (pålegg 3). Kombinasjonen av lovbruddene innenfor disse kategoriene gir i sum et utilstrekkelig konfidensialitetsvern. Overtredelsesgebyret bygger på en samlet vurdering av samtlige identifiserte lovbrudd.

Som nevnt i punkt 9, anser vi hovedfunnene i tilsynet (det samlede resultatet) for å være at NAV har organisert seg slik at et stort antall ansatte jobber med saker fra hele landet, innen flere tjenesteområder, og følgelig har tilsvarende vide tilganger. Samtidig er det ikke etablert noen systematisk kontroll av ansattes bruk av fagsystemene. Resultatet av dette er, slik vi ser det, at bruken av fagsystemene i stor grad er tillitsbasert. Manglende rutiner og styring gjør at ansatte ikke har verktøyene de trenger for å forvalte den tilliten og det ansvaret de gis.

NAV har vist til EDPBs *Guidelines 04/2022* kapittel 3 og 4 om utmåling av overtredelsesgebyr, som tematiserer konkurrence. Vi tolker henvisningen dit hen at NAV mener Datatilsynet har anvendt bestemmelsene som er overtrådt i konkurrence ved utmålingen av overtredelsesgebyret. Det er ikke er tilfellet. Imidlertid har vi ansett det hensiktsmessig å vurdere momentene som skal tillegges særlig vekt etter artikkel 83 nr. 2 bokstav a til k opp mot ulike elementer i overtredelsene av artikkel 24, 32 og 5.

Samtlige lovbrudd i den foreliggende tilsynssaken har negativ innvirkning på NAVs etterlevelse av det samme kravet – kravet til tilfredsstillende sikring av konfidensialitet.

Plikten til sikring av konfidensialitet for personopplysninger er regulert i flere ulike bestemmelser i personvernforordningen. Flere av disse lovkravene er brutt i den foreliggende saken. Læren om ulikeartet idealkonkurrens⁸ tilsier derfor at det skal utmåles ett samlet gebyr for overtredelsene, slik vi har gjort.

13.3 Skyldkravet

Ileggelse av overtredelsesgebyr er betinget av at den behandlingsansvarlige har utvist skyld i form av uaktsomhet eller forsett, jf. personvernforordningen artikkel 83 nr. 2 bokstav b, sammenholdt med artikkel 83 nr. 3, jf. EU-domstolens avgjørelser datert 5. desember 2023 i sakene C-807/21 (*Deutsche Wohnen*) og C-683/21.

NAV har bemerket at vurderingen av skyld må knyttes til nærmere angitte faktiske forhold som utgjør hvert enkelt lovbrudd. Videre har NAV anført at anonyme og kumulative feil bare kan føre til skyld i form av uaktsomhet, ikke i form av forsett. NAV bestrider at de har utvist forsett ved overtredelsene.

Vi nevner for ordens skyld at NAVs kommentarer knytter seg til varselet om vedtak, hvor skyldkravet var hjemlet i forvaltningsloven § 46. I henhold til avgjørelsen i sak C-807/21 (*Deutsche Wohnen*), som falt etter Datatilsynets varsel om vedtak, må skyldkravet hjemles direkte i personvernforordningen artikkel 83. Datatilsynet legger til grunn at tersklene for uaktsomhet og forsett de samme etter EU-retten som i norsk rett, slik at denne overgangen ikke har betydning for den materielle vurderingen.

Datatilsynet ser at det er behov for å nyansere vår vurdering av skyldkravet. Vi finner det imidlertid ikke riktig eller hensiktsmessig å vurdere graden av skyld opp mot hvert av lovbruddene isolert sett. De enkeltstående lovbruddene er elementer som på ulike måter påvirker NAVs konfidensialitetsvern i utførelsen av sitt samfunnsoppdrag. Skyldkravet vurderes her opp mot den manglende ivaretagelsen av konfidensialitetsvernet, basert på tilsynets hovedfunn, jf. punkt 13.2 ovenfor.

Datatilsynet presiserer at spørsmålet om det er utvist forsett i den foreliggende saken ikke har avgjørende betydning, ettersom Datatilsynet mener det må være på det rene at det uansett foreligger skyld i form av uaktsomhet. Skyldkravet etter artikkel 83 er dermed oppfylt. Vurderingen av om det foreligger forsett eller uaktsomhet har imidlertid betydning for den videre drøftelsen av hvorvidt overtredelsesgebyr skal ilegges, og overtredelsesgebyrets størrelse, jf. artikkel 83 nr. 2.

Forsett er definert slik i straffeloven § 22:

⁸ Se nettsiden <https://jusinfo.no/strafferett/konkurrens/ulikeartet-idealkonkurrens/>.

«§ 22.Forsett

Forsett foreligger når noen begår en handling som dekker gjerningsbeskrivelsen i et straffebud

- a. med hensikt,
- b. med bevissthet om at handlingen sikkert eller mest sannsynlig dekker gjerningsbeskrivelsen, eller
- c. holder det for mulig at handlingen dekker gjerningsbeskrivelsen, og velger å handle selv om det skulle være tilfellet.»

Uaktsomhet er definert slik i straffeloven § 23:

«§ 23.Uaktsomhet

Den som handler i strid med kravet til forsvarlig opptreden på et område, og som ut fra sine personlige forutsetninger kan bebreides, er uaktsom.

Uaktsomheten er grov dersom handlingen er svært klanderverdig og det er grunnlag for sterk bebreidelse.»

Datatilsynet har kommet til at den riktige skyldformen i denne saken er forsett. Med dette mener vi ikke at det foreligger forsett relatert til hvert av de 12 lovbruddene isolert sett, men til det faktum at NAV beviselig har hatt kunnskap om at konfidensialitetsvernet i virksomheten er utilstrekkelig på grunn av manglende rutiner, tilgangsstyring og loggkontroll (jf. punkt 10 ovenfor).

Hovedfunnene i det foreliggende tilsynet er de samme som ble konstatert gjennom tilsyn i 2007, 2010 og 2011. Dette gjelder særlig manglene knyttet til tilgangsstyring og loggkontroll. Vi må legge til grunn at NAV har en systematikk som gjør at denne kunnskapen fanges opp og at ansvar fordeles. Vi mener derfor at graden av kunnskap og bevissthet hos NAV om at de, ved å unnlate å gjøre noe med situasjonen over flere år, brøt loven, tilsier at det er utvist forsett, i det minste i form av såkalt eventualitetsforsett som kommer til uttrykk i straffeloven § 22 bokstav c. Etter dette har vi kommet til at NAV har utvist forsett.

NAV har anført at skyldgraden forsett forutsetter at det kan utpekes enkeltpersoner som har skyld i overtredelsene.

EU-domstolen konstaterte i sak C-807/21 (*Deutsche Wohnen*) at et krav om individualisering av skyld vil være i strid med personvernforordningen (se dommens avsnitt 46 flg.). Ettersom forsett er en aktuell skyldform etter personvernforordningen artikkel 83, må dommen forstås slik at anonyme og kumulative feil kan utgjøre grunnlag for skyld både i form av uaktsomhet og forsett. Dette er i samsvar med personvernforordningen hvoretter juridiske personer kan utvise forsett, jf. artikkel 83 nr. 2 bokstav b, jf. forordningen fortalepunkt 148.

Etter vårt syn ville det heller ikke være logisk å oppstille en regel hvor anonyme og kumulative feil kan lede til skyld i form av uaktsomhet, men ikke forsett.

Både uaktsomhet og forsett forutsetter en grad av bebreidelse eller «ond vilje». Det er en glidende overgang mellom uaktsomhet og forsett, hvor det avgjørende er graden av bevissthet om at handlingene en foretar seg oppfyller lovens objektive vilkår for straff.

Høyesterett uttaler i HR-2022-1271-A, avsnitt 48-50:

«(48) De rettssikkerhetsgarantier for siktede som praksis fra EMD bygger på, er ivaretatt der det foreligger anonyme og kumulative feil. Også ved slike feil vil det være mulig å imøtegå en anklage om at noen som har handlet på vegne av foretaket, har opptrådt uaktsomt. (...)

(49) Ved å akseptere anonyme og kumulative feil unngår man at krav om individualisering av skyld reduserer effektiviteten av foretaksstraffen, som i vårt land spiller en viktig rolle i håndhevelsen av regelverk som gjelder for offentlig og privat virksomhet. Man unngår dessuten at to eller flere foretak som har utvist den samme form for straffbar adferd, blir behandlet forskjellig avhengig av om det kan bringes på det rene hvilke personer som har foranlediget de aktuelle forhold.

(50) Jeg kan på denne bakgrunn ikke se at det vil være i strid med EMK å ilegge foretaksstraff ved anonyme og kumulative feil.»

Slik vi forstår Høyesteretts uttalelser, er åpningen for at anonyme og kumulative feil kan utgjøre grunnlag for ansvar ikke forbeholdt en bestemt ansvarsform. Det vil heller ikke være en god regel dersom forsettlige lovovertridelser skal sanksjoneres mindre effektivt enn uaktsomme lovovertridelser. Det ville uthule muligheten for å differensiere reaksjonen på lovbrudd ut fra skyldgraden, og på den måten premiere tilfeller hvor det er utvist en høy grad av «ond vilje».

Datatilsynet fastholder etter dette at det ikke er en forutsetning for skyldgraden forsett at det kan utpekes enkeltpersoner som har skyld i overtredelsene.

13.4 Vurderingsmomenter som skal tillegges særlig vekt

Forordningen artikkel 83 nr. 2 bokstav a til k oppstiller momenter som skal tas hensyn til ved avgjørelsen om hvorvidt det skal ilegges overtredelsesgebyr samt overtredelsesgebyrets størrelse. Under følger vår vurdering av de momentene vi anser som relevante i vurderingen av om overtredelsesgebyr skal ilegges.

13.4.1 Vurdering av artikkel 83 nr. 2 bokstav a

Forordningen artikkel 83 nr. 2 bokstav a lyder som følger:

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd

NAV har brutt grunnleggende prinsipper for behandling av personopplysninger gjennom overtredelsene av artikkel 5 nr. 1 bokstav f og artikkel 5 nr. 2. Overtredelsene av artikkel 24 og 32 nr. 1, 2 og 4 viser en gjennomgripende systemsvakhet og mangelfull kontroll knyttet til personopplysningssikkerhet som sikrer konfidensialitet og forpliktelsene NAV har som behandlingsansvarlig, både i rutiner og i praksis. Overtredelsene indikerer at NAV ikke har sett på ansatte som en risikofaktor ved vurderinger knyttet til personopplysningssikkerhet.

I tilsynet har vi sett på utvalgte systemer i den statlige delen av NAVs tjenesteyting. Datatilsynet legger til grunn at behandlingsformålene i systemene knytter seg til forvaltning av befolkningens rettigheter etter velferdslovgivningen. Mange av disse rettighetene er til for personer i sårbare livssituasjoner.

Overtredelsene er omfattende og har pågått over mange år, jf. punkt 10 ovenfor. Et svært stort antall registrerte er berørt. Vi viser til at NAV i 2022 hadde ca. 3,2 millioner tjenestemottakere.

Når det gjelder omfanget av den skade de registrerte har lidd, har vi i hovedsak undersøkt skaderisikoen. Manglende styring fra ledelsen, svært vide tilganger for ansatte og fravær av loggkontroll medfører stor risiko for skade i form av at ansatte uberettiget tilegner seg personopplysninger. Vi har ikke undersøkt i hvilken utstrekning denne risikoen faktisk har realisert seg. Omfanget av den skade de registrerte har lidd er derfor ikke kjent.

Imidlertid anser vi det som en klar integritetskrenkelse overfor de registrerte at personopplysningene deres er tilgjengelig for et langt større antall ansatte enn de som har tjenstlig behov for disse.⁹ Dette er et alvorlig brudd på konfidensialitetsprinsippet nedfelt i personvernforordningen artikkel 5 nr. 1 bokstav f.

Overtredelsenes karakter, alvorlighetsgrad og varighet trekker i skjerpene retning.

13.4.2 Vurdering av artikkel 83 nr. 2 bokstav b

Forordningen artikkel 83 nr. 2 bokstav b lyder som følger:

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

⁹ Endret etter følgende kommentar fra NAV 4. januar 2024:

«Vi bestrider ... at personopplysninger «*ligger mer eller mindre åpent tilgjengelig for alle ansatte i NAV*» som Datatilsynet skriver i punkt 8.2.3. bokstav a). Dette utgjør dermed ikke en «klar integritetskrenkelse»».

Datatilsynets vurdering av skyldkravet fremkommer av vedtaket punkt 13.3 ovenfor. Vi har kommet til at NAV har utvist forsett ved overtredelsene. Forsett ved overtredelsene tillegges vekt i skjerpende retning.

13.4.3 Vurdering av artikkel 83 nr. 2 bokstav c

Forordningen artikkel 83 nr. 2 bokstav c lyder som følger:

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd

NAVs sikkerhetsrammeverk er under revidering og skal ferdigstilles i 2026. Vi legger til grunn dette at dette arbeidet i fremtiden vil bøte på overtredelsene av artikkel 24.

Arbeidet med sikkerhetsrammeverket kan også begrense noe av skaden som følger av overtredelsene av artikkel 5 og 32. Likevel oppfatter vi ikke at NAV har hatt noen intensjon om å begrense ansattes tilganger i fagsystemene eller å innføre systematisk loggkontroll.¹⁰ Vi kan derfor ikke vektlegge dette planlagte tiltaket i formildende retning når det gjelder begrensning av skadepotensialet som følger av de påviste lovbruddene.

13.4.4 Vurdering av artikkel 83 nr. 2 bokstav d

Forordningen artikkel 83 nr. 2 bokstav d lyder som følger:

d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32

Overtredelsene i denne saken går nettopp ut på at NAV ikke har gjennomført tilstrekkelig egnede tekniske og organisatoriske tiltak for å sikre at behandlingen av personopplysninger utføres lovlig. Det foreligger derfor i utgangspunktet en høy grad av ansvar.

Når det gjelder manglene knyttet til tilgangsstyring og loggkontroll, jf. artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4, er graden av ansvar særlig høy, ettersom NAV har blitt gjort oppmerksom på overtredelsene flere ganger tidligere – og i tillegg ikke har innrettet seg etter pålegg om å utbedre forholdene, jf. punkt 9.1, 9.2 og 9.3 ovenfor. Se også bokstav e og i nedenfor.

¹⁰ NAV skriver i kommentarene av 4. januar 2024: «Vi kjenner oss ikke igjen i Datatilsynets beskrivelse av NAVs manglende intensjon i arbeidet med tilgangsstyring og logging (...). Hovedtiltaket for å begrense ansattes tilgang til saksopplysninger er å erstatte de gamle fagsystemene». Datatilsynet fastholder vår oppfatning på dette punktet. Erstatning av gamle fagsystemer vil ikke forbedre konfidensialitetsvernet med mindre det medfører begrensninger i de ansattes tilganger. Det har ikke NAV vist noen intensjon om. Tvert imot har NAV bestridt pålegg 2, som omhandler nettopp dette. Når det gjelder innføring av systematisk loggkontroll, oppfatter vi at NAV, etter at vi varslet vedtak i saken, har til hensikt å innføre dette.

Som nevnt, oppfatter vi at NAV ikke har hatt noen intensjon om å begrense ansattes tilganger i fagsystemene eller innføre systematisk loggkontroll.¹¹ Vi har inntrykk av at NAV har etablert flere tekniske muligheter for begrensnng av tilganger, men at disse i svært begrenset grad er i bruk. Dette gjelder for eksempel fagsystemet Arena. Det fremgikk under tilsynet at «utvidbar»-rollene i Arena, hvor ansatte skriftlig må begrunne oppslag utenfor kjernetilganger, ikke lenger kan brukes som forutsatt. NAV har over tid endret organiseringen av oppgaveløsningen slik at det ikke lenger er naturlig å bruke tekniske avgrensninger knyttet til f.eks. geografi.

Vi mener at NAV gjennom dette har utvist en manglende evne til å gjennomføre nødvendige forbedringer av personopplysningsikkerheten, på tross av kjennskapet til at det medfører lovovertrredelser. Det er derfor ingen tvil om at graden av ansvar må tillegges vekt i skjerpnde retning.

13.4.5 Vurdering av artikkel 83 nr. 2 bokstav e

Forordningen artikkel 83 nr. 2 bokstav e lyder som følger:

e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren

Vi har ikke tidligere kontrollert NAVs overholdelse av artikkel 24. Når det gjelder overtredelsen av denne bestemmelsen, foreligger derfor ingen tidligere kjente overtredelser som anses relevante for saken.

Når det gjelder overtredelsene av artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4 gjennom mangelfull tilgangsstyring og loggkontroll, foreligger flere relevante tidligere overtredelser. Vi viser til at det på disse punktene ble konstatert lovbrudd gjennom tilsyn i 2007, 2010 og 2011, jf. punkt 10.1, 10.2 og 10.3 ovenfor. Overtredelsene knytter seg til bestemmelser i personopplysningsloven (2000) som nå er videreført gjennom artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4. Dette tillegges vekt i skjerpnde retning.

13.4.6 Vurdering av artikkel 83 nr. 2 bokstav f

Forordningen artikkel 83 nr. 2 bokstav f lyder som følger:

f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den

NAV har gjennom hele tilsynsprosessen opptrådt imøtekommende og samarbeidsvillig. NAV har overholdt frister og fremlagt etterspurt informasjon i en systematisk og ryddig form. Overholdelse av den lovpålagte plikten til å fremlegge all informasjon tilsynsmyndigheten

¹¹ Se fotnote 10.

trenger for å utføre sine oppgaver, jf. artikkel 58 nr. 1, kan imidlertid ikke tillegges vekt i formidlende retning, jf. Personvernemndas avgjørelse i PVN-2022-03.

13.4.7 Vurdering av artikkel 83 nr. 2 bokstav g

Forordningen artikkel 83 nr. 2 bokstav g lyder som følger:

g) kategoriene av personopplysninger som er berørt av overtredelsen

Fagsystemene hos NAV kan inneholde eller gi tilgang til detaljerte opplysninger om bl.a. familierelasjoner, helse, utdanning, arbeidsforhold, økonomi, tro og etnisitet, institusjonsopphold, straffedommer og lovovertridelser. Informasjon om hvilke av NAVs ytelser en mottar kan i seg selv være en helseopplysning. Fagsystemene har ingen tidsmessig avgrensning, slik at ansatte får tilgang til informasjon om enkeltpersoner fra alle faser i livet. Flere av opplysningene som er berørt av overtredelsene utgjør særlige kategorier personopplysninger i henhold til artikkel 9 nr. 1.

Disse momentene tillegges vekt i skjerpende retning.

13.4.8 Vurdering av artikkel 83 nr. 2 bokstav h

Forordningen artikkel 83 nr. 2 bokstav h lyder som følger:

h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen

Datatilsynet fikk kjennskap til overtredelsene gjennom det stedlige tilsynet og pålegg til NAV om å fremlegge relevant informasjon.

Overtredelsene gjelder i stor grad systematiske, organisatoriske svakheter som NAV selv ikke har ansett som avvik. I samtaler med NAV har deres representanter lagt vekt på å forklare hvorfor systemene må innrettes slik de er. En kan med dette ikke si at NAV har underrettet Datatilsynet om overtredelsene. Vi finner likevel ikke grunnlag for å tillegge dette vurderingsmomentet vekt i skjerpende retning.

13.4.9 Vurdering av artikkel 83 nr. 2 bokstav i

Forordningen artikkel 83 nr. 2 bokstav i lyder som følger:

i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes

Det har ikke tidligere vært gjennomført tiltak overfor NAV med hensyn til overtredelse av artikkel 24.

NAV ble ilagt pålegg fra Datatilsynet om å etablere tilfredsstillende personopplysningssikkerhet gjennom tilgangsstyring, logging og loggkontroll i 2007, 2010 og 2011. Vi viser til punkt 10.1, 10.2 og 10.3 ovenfor. Påleggene knytter seg til bestemmelser i personopplysningsloven (2000) som nå er videreført gjennom artikkel 5 nr. 1 bokstav f og artikkel 32 nr. 1, 2 og 4. Vi mener derfor at påleggene, både faktisk og rettslig, knytter seg til «samme saksgjenstand», jf. bokstav i.

Pålegget om å etablere logging fra vedtak i 2010 anses som overholdt. På områdene tilgangsstyring og loggkontroll vurderer vi dagens tilstand som tilsvarende eller forverret siden forrige tilsyn.¹² Påleggene om å etablere tilfredsstillende tilgangsstyring og loggkontroll anses dermed ikke overholdt. Dette tillegges vekt i skjerpene retning.

13.4.10 Vurdering av artikkel 83 nr. 2 bokstav j

Forordningen artikkel 83 nr. 2 bokstav j lyder som følger:

j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42

Dette momentet er ikke relevant for saken.

13.4.11 Vurdering av artikkel 83 nr. 2 bokstav k

Forordningen artikkel 83 nr. 2 bokstav k lyder som følger:

k) enhver annen skjerpene eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen

Vi legger i formildende retning vekt på at NAV gir de registrerte innsyn i logg over ansattes oppslag i fagsystemene. Dette kan riktignok ikke anses som et sikkerhetstiltak, men kan ha en viss preventiv effekt.

I skjerpene retning legger vi vekt på at NAV, i kraft av sin rolle, har et særlig ansvar for å forsikre seg om at personopplysninger behandles lovlig.

I tillegg legger vi i skjerpene retning vekt på at det i stor grad er overlatt til den registrerte å oppdage ulovlige oppslag i fagsystemene.

13.4.12 Samlet vurdering

Det er et lederansvar å sørge for at personvernet ivaretas tilstrekkelig i en virksomhet. Lovbruddene som er avdekket viser strukturelle, organisatoriske svakheter og en manglende

¹² Se fotnote 6.

styring av og forståelse for betydningen av personvern og hvilke forventninger som stilles til NAV på dette området. Vi vurderer det som svært alvorlig at en myndighet som NAV ikke i tilstrekkelig grad har behandlet befolkningens personopplysninger på en lovlig måte.¹³ Det er tydelig at arbeidet med personopplysningssikkerhet ikke er gitt tilstrekkelig prioritet og ressurser.

Slik styringssystemet knyttet til tilgangsstyring og loggkontroll er innrettet i dag, er det svært krevende å etterprøve om bruken av fagsystemene skjer innenfor lovens rammer. Lokale kontorer er gitt stor frihet til å organisere seg på egne måter. Det medfører at NAVs styringsprinsipp om «tjenstlig behov» i praksis defineres langt nede i organisasjonen. Det fører til at ledelsen tilsynelatende i stor grad har fraskrevet seg både ansvaret for og muligheten til å kontrollere etterlevelsen av personvernforordningen i praksis. Manglende styring medfører en høy risiko for at etterlevelse beror på tilfeldigheter. Det er ikke akseptabelt for en myndighet som NAV.

Etter en samlet vurdering har Datatilsynet kommet til at NAV skal ilegges et overtredelsesgebyr. Tidligere pålegg fra Datatilsynet har vist seg ikke å være tilstrekkelig virkningsfulle. Ileggelse av overtredelsesgebyr anses derfor nødvendig.

13.5 Utmåling av gebyret

De samme momentene som ved vurdering av om gebyr skal ilegges, skal tillegges vekt også ved utmålingen. Overtredelsesgebyret skal i henhold til artikkel 83 nr. 1 være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Dette innebærer at tilsynsmyndigheten skal gjøre en konkret, skjønnsmessig vurdering i hvert enkelt tilfelle.

NAV har brutt grunnleggende prinsipp for behandling av personopplysninger, jf. artikkel 83 nr. 5 bokstav a, jf. artikkel 5 nr. 1 bokstav f og artikkel 5 nr. 2. Det er dermed grunnlag for å ilegge NAV et overtredelsesgebyr på inntil 20 000 000 euro (p.t. ca. 230 000 000 kroner).

I vurderingen av gebyrets størrelse, har vi vektlagt at NAV har tilgjengeliggjort særlige kategorier personopplysninger i svært lang tid om et høyt antall personer, uten at nødvendige sikkerhetsmekanismer er etablert.

Vi legger også vekt på at NAV ikke har reagert adekvat på gjentatte oppfordringer, gjennom tilsyn og eksterne evalueringer, om å gi arbeidet med personopplysningssikkerhet den nødvendige prioritet. Denne omstendigheten er relevant ved flere av vurderingsmomentene som i henhold til artikkel 83 nr. 2 skal tillegges særlig vekt, herunder vurderingene av ansvars- og skyldgrad.

¹³ NAV skriver i kommentarene av 4. januar 2024 at de, ut fra sine anførsler knyttet til sakens omfang og sakens opplysning, er «uenig i at Datatilsynet har et godt nok grunnlag for slutningen om at NAV har en «manglende forståelse for betydningen av personvern og hvilke forventninger som stilles til NAV på dette området». Datatilsynet fastholder vurderingen og viser til punkt 7 ovenfor.

Overtredelsene er gjennomgripende, og er meget alvorlige, sett i lys av at behandling av personopplysninger er en sentral del av NAVs virksomhet og at det derfor må stilles særlig høye krav til at NAV ivaretar personopplysninger på en sikker måte.

I formildende retning har vi kun funnet å se hen til at NAV har et pågående arbeid med å revidere sikkerhetsrammeverket, samt at NAV gir registrerte personer logginnsyn.

Etter en totalvurdering av de ovennevnte momentene, og sett hen til at lovverkets krav om at ileggelsen av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende, har vi kommet til at et overtredelsesgebyr på 20 000 000 – tjue millioner – kroner anses riktig. Ved utmålingen har vi tatt hensyn til at også påleggene som er varslet i punkt 4 vil medføre en økonomisk belastning.

Reglene for utmåling av overtredelsesgebyr er i utgangspunktet like for offentlige og private aktører. På grunn av alvorlighetsgraden i denne saken, sammenlignet med andre saker hvor Datatilsynet har ilagt overtredelsesgebyr, finner vi det nødvendig å forklare hvorfor gebyret ikke er satt høyere.

Forordningen artikkel 83 nr. 7 åpner for at det i nasjonal rett kan fastsettes regler om «når og i hvilken grad» offentlige myndigheter kan ilegges overtredelsesgebyr. I personopplysningsloven § 26 andre ledd er det bestemt at offentlige myndigheter kan ilegges overtredelsesgebyr på lik linje som private aktører.

I høringen til personopplysningsloven (2018) tok flere høringsinstanser til orde for at overtredelsesgebyrene som kan ilegges offentlige myndigheter bør begrenses beløpsmessig. Forklaringen på at denne muligheten ikke ble benyttet, er uttrykt slik i forarbeidene¹⁴:

«Departementet har notert seg bekymringen som enkelte offentlige høringsinstanser har uttrykt, men departementet legger til grunn at det innenfor reglene i forordningen artikkel 83, som også angir de momenter det skal legges vekt på ved utmålingen av administrative gebyrer, ligger rom for et betydelig skjønn med hensyn til størrelsen på gebyret. Beløpsgrensene i forordningen artikkel 83 angir maksimalgrenser for utmåling av administrative gebyrer, mens det ikke er fastsatt noen minimumsgrenser.»

Vi tolker dette dit hen at meningen fra lovgivers side har vært å legge til rette for en ulik utmålingspraksis overfor offentlige og private aktører.

I tillegg medfører kriteriene i artikkel 83 nr. 1 om at overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfullt og avskrekkende, etter vårt syn, at utmålingen bør slå ut ulikt for offentlige og private aktører. Til sammenligning er det i Sverige innført en beløpsmessig grense på SEK 10 000 000 for offentlige myndigheter, se kapittel 6 § 2 i Lag (2018:218) med kompletterende bestämmelser till EU:s dataskyddsförordning. I fraværet av en slik grense i norsk rett, har vi i denne saken ansett det nødvendig å vedta et forholdsvis høyt gebyr.

¹⁴ Prop.56 LS (2017-2018) s. 142.

Samtidig vil vi understreke at overtredelser av tilsvarende alvorlighetsgrad hos en privat aktør kunne ført til et langt høyere gebyr enn det vi har kommet frem til i den foreliggende saken.

14. Klageadgang

NAV kan klage på dette vedtaket. En eventuell klage må sendes til Datatilsynet **innen tre uker** fra mottak av dette vedtaket jf. forvaltningsloven §§ 2, 28 og 29. Dersom vi etter vurdering av fremsatt klage opprettholder vårt vedtak vil vi sende saken videre til Personvernemnda for klagebehandling.

Dersom dere ikke påklager vedtaket om overtredelsesgebyr, er oppfyllelsesfristen fire uker etter klagefristens utløp, jf. personopplysningsloven § 27.

Ved spørsmål kan dere kontakte Ingrid H. Espolin Johnson på telefon 22 39 69 42, eller e-post ingrid.johnson@datatilsynet.no.

15. Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter, jf. forvaltningsloven § 18. Vi informerer også om at alle dokumentene i utgangspunktet er offentlige, jf. offentlighetsloven § 3.

Med vennlig hilsen

Line Coll
direktør

Ingrid H. Espolin Johnson
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: ARBEIDS- OG VELFERDSETATEN, Anders Holt
ARBEIDS- OG VELFERDSETATEN, Trond Eirik Schea

Vedlegg: Endelig tilsynsrapport