Datatilsynet

ARBEIDS- OG VELFERDSETATEN
Postboks 354
8601 MO I RANA

Deres referanse	Vår referanse	Dato
23/4873	23/00708-23	27.11.2023

Oversendelse av endelig tilsynsrapport – Varsel om vedtak om pålegg og overtredelsesgebyr

1. Innledning

Vi viser til stedlig tilsyn hos Arbeids- og velferdsetaten (NAV) 6. september 2023, som ble varslet i vårt brev av 1. mars 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.

Foreløpig tilsynsrapport ble oversendt NAV 1. november 2023. NAV innga sine merknader til rapporten 22. november 2023.

2. Endelig tilsynsrapport og varsel om vedtak

Vår endelige tilsynsrapport følger vedlagt. På bakgrunn av NAVs merknader har vi gjort enkelte endringer i rapporten. Endringene er markert løpende med fotnoter.

I tilsynet har vi kontrollert om NAV sikrer tilfredsstillende konfidensialitet i IT-løsningene («fagsystemene») som benyttes til å behandle personopplysninger i forbindelse med tjenesteyting.

Kontrollen omfattet 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 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 i praksis heller ikke er tilfredsstillende.

I rapporten har vi identifisert 12 lovbrudd (i rapporten og i varselet her også omtalt som «avvik») som NAV pålegges å rette opp i.

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

Vurderingene våre og de faktiske og rettslige forholdene som ligger til grunn for de varslede påleggene og det varslede overtredelsesgebyret, fremgår nedenfor.

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.

3. Varsel om vedtak om pålegg

I samsvar med forvaltningsloven § 16 varsler vi med dette at vi med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d, vurderer å fatte følgende vedtak:

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:

   a. *Rutiner 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.*

   b. *Rutine 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.*

c. *Rutine 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.*

d. *Oppdaterte 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.*

e. *Rutine for kontroll av enhetslederes 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.*

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.*

   Herunder må NAV etablere:

   a. *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.*

   b. *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.*

   c. *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.*

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.*

Datatilsynet ber om en tidsplan for gjennomføring av de varslede påleggene, som vil bli vurdert hensyntatt under utformingen av det endelige vedtaket.

4. Varsel om vedtak om ileggelse av overtredelsesgebyr

I samsvar med forvaltningsloven § 16 varsler vi med dette at vi med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, vurderer å fatte 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.*

5. 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. Nesten alle innbyggere i Norge er i kontakt med NAV i løpet av livet.

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

Det ligger derfor en innebygd høy personvernrisiko i NAVs virksomhet, som medfører strenge krav til personopplysningssikkerheten.

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.

6. Overordnede funn

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.

Vi har, som nevnt, identifisert 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 enhetslederes 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.

Vi observerte under tilsynet at NAVs sikkerhetsrammeverk er under revidering. NAV har et mål om å sluttføre 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.

7. Tidligere tilsyn og evalueringer mv.

7.1 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.

7.2 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.»*

7.3 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 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.

7.4 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.[1] 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.»*

7.5 PwCs evaluering av NAV i 2020

I 2020 gjennomførte PwC AS en modenhetsvurdering[2] 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.

7.6 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.

7.7 Avsluttende merknad – tidligere tilsynsbetydning 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. I vår vurdering av nødvendigheten av å 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.

8. Overtredelsesgebyr

8.1 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.

---

[1] *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.

[2] *Modenhetsvurdering sikkerhet* (november 2020), PwC AS. Rapporten er unntatt offentlighet.

Det er kun overtredelser av bestemmelsene som er oppregnet i artikkel 83 nr. 4 og 5 som kan sanksjoneres med overtredelsesgebyr, jf. lovkravet i forvaltningsloven § 44 første ledd.

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.

Etter forvaltningsloven § 46 første ledd kreves subjektiv skyld (uaktsomhet) hos den eller de som har opptrådt på vegne av foretaket ved ileggelse av overtredelsesgebyr, med mindre noe annet er bestemt.

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.

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.

8.2 Vurdering av om overtredelsesgebyr skal ilegges

8.2.1 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.

Det foreligger dermed flere lovbrudd som kan gi grunnlag for ileggelse av overtredelsesgebyr, jf. forvaltningsloven § 44 første ledd.

8.2.2 Skyldkravet

Datatilsynet kan ikke utpeke enkeltpersoner hos NAV som har skyld i overtredelsene. Ut fra rettspraksis er det imidlertid ikke et krav om at skylden individualiseres. Både anonyme og kumulative feil kan utgjøre grunnlag for ansvar ved ileggelse av foretaksstraff, jf. HR-2022-1271-A, avsnitt 46-50.

Som vist ovenfor i punkt 7, knytter overtredelsene seg til forhold som NAV flere ganger har blitt gjort oppmerksom på at ikke oppfyller lovens krav. NAV har vært kjent med dette i lang tid. Vi må ut fra dette konkludere med at det har vært et bevisst valg fra NAVs side å gå videre med tekniske og organisatoriske løsninger som ikke oppfyller kravene i personvernregelverket. NAV har dermed utvist forsett ved overtredelsene. Skyldkravet etter forvaltningsloven § 46 er således oppfylt, ettersom alminnelig uaktsomhet uansett er tilstrekkelig.

8.2.3 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;

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 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. Dataminimeringsprisnippet synes ikke hensyntatt gjennom NAVs styringsprinsipp om «tjenstlig behov».

Overtredelsene er omfattende og har pågått i mange år, trolig helt siden opprettelsen av NAV, jf. punkt 7 ovenfor. Et svært stort antall registrerte er berørt. Vi viser til at NAV i 2022 hadde ca. 3,2 millioner tjenestemottakere.

I tilsynet har vi sett på utvalgte systemer i den statlige delen av NAVs tjenesteyting. Vi har ikke grunnlag for å vurdere formålene med hver enkelt behandling. Generelt legger vi til grunn at behandlingsformålene knytter seg til forvaltning av befolkningens rettigheter etter velferdslovgivningen. Mange av disse rettighetene er til for personer i sårbare livssituasjoner.

Når det gjelder omfanget av den skade de registrerte har lidd, har vi kun 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 ligger mer eller mindre åpent tilgjengelig for alle ansatte i NAV. Dette er et alvorlig brudd på konfidensialitetsprinsippet nedfelt i personvernforordningen artikkel 5 nr. 1 bokstav f.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Vi har kommet til at NAV har utvist forsett ved overtredelsene, jf. punkt 8.2.2 ovenfor. Dette tillegges vekt i skjerpende retning.

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 noen intensjon om å begrense ansattes tilganger i fagsystemene eller å innføre systematisk loggkontroll. Vi kan derfor ikke vektlegge dette tiltaket i formildende retning når det gjelder begrensning av skade som følge av overtredelsene på disse områdene.

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 overtredelsene av 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 7.1, 7.2 og 7.3 ovenfor. Se også bokstav e og i nedenfor.

Som nevnt, oppfatter vi at NAV ennå ikke har noen intensjon om å begrense ansattes tilganger i fagsystemene eller innføre systematisk loggkontroll. Vi har inntrykk av at NAV har etablert flere tekniske muligheter for begrensning 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 personopplysningssikkerheten, på tross av kjennskapen til at det medfører lovovertredelser. Det er derfor ingen tvil om at graden av ansvar trekker i skjerpende retning.

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 7.1, 7.2 og 7.3 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 skjerpende retning.

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

Som beskrevet under bokstav h nedenfor, har NAV selv ikke ansett overtredelsene som avvik. Vurderingsmomentet i bokstav f har derfor ikke kommet på spissen i denne saken. Vi finner ikke grunnlag for å vektlegge dette momentet.

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 lovovertredelser. 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.

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.

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 7.1, 7.2 og 7.3 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. Påleggene om å etablere tilfredsstillende tilgangsstyring og loggkontroll anses dermed ikke overholdt. Dette tillegges vekt i skjerpende retning.

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

Ikke relevant for saken.

k) enhver annen skjerpende 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 skjerpende retning legger vi vekt på at NAV, i kraft av sin rolle, har et særlig ansvar for å forsikre seg om at personopplysninger behandles på en sikker måte. 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.

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

8.2.4 Samlet vurdering

Lovbruddene som er avdekket viser strukturelle, organisatoriske svakheter og en manglende 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 ivaretatt befolkningens personopplysninger på en sikker måte. Det er tydelig at arbeidet med personopplysningssikkerhet ikke er gitt tilstrekkelig prioritet og ressurser. Det er et lederansvar å sørge for at personvernet ivaretas tilstrekkelig i en virksomhet.

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. Vi har i denne vurderingen sett hen til at tidligere pålegg har vist seg ikke å være tilstrekkelig virkningsfulle. Ileggelse av overtredelsesgebyr anses derfor nødvendig.

8.3 Utmåling av gebyret

De samme momentene som ved vurdering av om gebyr skal ilegges, skal tillegges særlig 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 NOK).

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 har også lagt vekt på at NAV har utvist forsett ved overtredelsene, bl.a. ved ikke å innrette seg etter tidligere pålegg knyttet til samme saksgjenstand. 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 3 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 forarbeidene[3]:

> *«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

[3] Prop.56 LS (2017-2018) s. 142.

grense på 10 000 000 SEK for offentlige myndigheter, se kapittel 6 § 2 i Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. I fraværet av en slik grense, har vi i denne saken ansett det nødvendig å vedta et forholdsvis høyt gebyr. Samtidig vil vi understreke at overtredelser av tilsvarende alvorlighetsgrad hos en privat aktør ville ført til et langt høyere gebyr enn det vi har kommet frem til i denne saken.

9. Videre saksgang

Dette er et forhåndsvarsel om vedtak om pålegg og overtredelsesgebyr, jf. forvaltningsloven § 16. Dersom dere har kommentarer til varselet, ber vi om at disse sendes oss **innen tre uker** etter mottak av dette brevet.

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

10. 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, Odd-Erik Røste

Vedlegg: Endelig tilsynsrapport