Datatilsynet

HELSEPLATTFORMEN AS
POSTMOTTAK, Postboks 1204 Torgard
7462 TRONDHEIM

Unntatt offentlighet:
Offl. § 13, jf. personopplysningsloven § 24 første ledd 2. punktum

Deres referanse	Vår referanse	Dato
	24/00696-12	28.11.2025

Oversender endelig tilsynsrapport - varsel om vedtak om pålegg

1. Innledning

Vi viser til det stedlige tilsynet Datatilsynet gjennomførte hos Helseplattformen AS (HP AS) den 22. mai – 23. mai 2024. Tilsynet ble gjennomført med hjemmel i personvernforordningen artikkel 57 nr. 1 bokstav a og h, jf. personopplysningsloven § 20, jf. også pasientjournalloven § 26.

Formålet med tilsynet var å undersøke om HP AS som dataansvarlig legger til rette for at behandling av personopplysninger i Helseplattformen (heretter Løsningen) skjer i tråd med kravene i personopplysningsloven og personvernforordningen samt pasientjournalloven.

Spesifikt undersøkte vi på overordnet nivå:

- omfanget av HP AS' dataansvar og deres systematikk for styring av arbeidet med personvern og personopplysningssikkerhet
- de tekniske og organisatoriske tiltakene for tilgangsstyring i løsningen Helseplattformen
- HP AS' avvikshåndtering og -oppfølging

Tilsynet er avgrenset mot forhold ved Løsningen som gjelder pasientsikkerheten, som følges opp av Statens helsetilsyn og Statsforvalteren i Trøndelag. Vi har heller ikke vurdert hvorvidt Løsningen er et godt og egnet arbeidsverktøy for helsepersonell.

Den endelige tilsynsrapporten følger vedlagt. Deres merknader til foreløpig rapport er innarbeidet i endelig rapport.

Vedlagt følger også endelige rapporter fra tilsynene med St. Olavs hospital HF (St. Olav) og Melhus kommune, som ble gjennomført henholdsvis 22. og 23 oktober 2024. Disse tilsynene ble gjennomført som ledd i tilsynet mot Helseplattformen AS som dataansvarlig for Løsningen. Eventuelle lovbrudd som er avdekket skyldes forhold som dekkes av Helseplattformen AS' dataansvar. Tilsynene med St. Olav og Melhus kommune hadde som formål å undersøke hvordan dataansvaret ble ivaretatt i praksis fra aktørenes perspektiv.

Vi har sett de tre tilsynene i sammenheng i våre vurderinger som ligger til grunn for vedtaksvarselet under.

2. Varsel om vedtak om pålegg

Vi har kommet til at det er vesentlige mangler ved de organisatoriske tiltakene HP AS har etablert, samt mangler ved enkelte tekniske tiltak, jf. personvernforordningen artikkel 24 og 32 og pasientjournalloven §§ 22 og 23.

Datatilsynet har forholdt seg til at HP AS fullt ut er dataansvarlig for tekniske og organisatoriske tiltak i Løsningen. Der er dermed HP AS som er ansvarlig for å etablere tilstrekkelige tiltak som er nødvendige for etterlevelse av personvernregelverket.

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d, jf. forvaltningsloven § 16, varsler vi følgende vedtak om pålegg:

> *Helseplattformen AS, org.nr. 922 307 814, pålegges å etablere egnede organisatoriske tiltak for å sikre tilfredsstillende personopplysningssikkerhet, jf. personvernforordningen artikkel 24 og 32 samt pasientjournalloven §§ 22 og 23. Tiltakene må etableres overfor henholdsvis helseforetakene og kommunene, tilpasset lokale forhold. Tiltakene skal sikre at aktørene settes i stand til å bruke Løsningen på en riktig og tilstrekkelig sikker måte.*
>
> *Blant annet må Helseplattformen AS:*
>
> - [redacted]
> - *Lage en handlingsplan overfor det enkelte helseforetak samt felles for kommunene der det planlegges for hvordan nødvendig informasjon skal tilgjengeliggjøres på en strukturert måte*
> - *Lage en tidsplan for gjennomføringen*
>
> *Helseplattformen AS pålegges å sende en tiltaksplan til Datatilsynet innen en nærmere angitt frist.*
>
> *Helseplattformen AS pålegges også å sende Datatilsynet en status for retting av enkelte forhold innen samme frist. I den grad problemene ikke er løst, må Helseplattformen AS oversende en tidsplan for arbeidet. Det gjelder følgende forhold (det relevante punktet i tilsynsrapporten er gjengitt i parentes):*
>
> - *HP AS' system for avvikshåndtering (punkt 7)*
> - [redacted]
> - *Arbeidslister – tilgjengeliggjøring ut fra lokasjon (punkt 9.3)*
> - *Manglende begrunnelse for enkeltoppslag (punkt 9.5)*
> - [redacted]

3. Datatilsynets korrigerende myndighet

Personvernforordningen artikkel 58 nr. 2 gir Datatilsynet til å beslutte egnede korrigerende tiltak mot behandlingsansvarlige der det foreligger brudd på forordningens regler.

Etter artikkel 58 nr. 2 bokstav d kan vi «pålegge den behandlingsansvarlige eller databehandleren å sørge for at behandlingsaktivitetene skjer i samsvar med bestemmelsene i denne forordning og, dersom det er relevant, på en bestemt måte og innen en bestemt frist».

4. Datatilsynets vurdering

4.1 Ansvarsforhold – rapportens punkt 5

Vi er kjent med at Helse- og omsorgsdepartementet evaluerer vedtaket om dataansvar av 22. mars 2022. Våre vurderinger knytter seg til vedtaket slik det forelå på tilsynstidspunktet.

Som det fremgår av våre vurderinger i punkt 5.3 i tilsynsrapporten, mener vi at det ikke er samsvar mellom dataansvaret slik det er formulert i vedtaket og de iverksatte organisatoriske tiltakene fra HP AS' side. Etter vår vurdering, har ikke HP AS ivaretatt dataansvaret når det gjelder behov for og plikt til å etablere organisatoriske tiltak, særlig overfor helseforetakene. Dette utgjør et brudd på dataansvarliges plikt til å etablere egnede organisatoriske tiltak for etterlevelse av personvernregelverket som følger av personvernforordningen artikkel 24, jf. pasientjournalloven § 23.

Vi mener at dette er verifisert gjennom særlig tilsynet med St. Olav, se punkt 5 i rapporten fra dette tilsynet. At ansvaret for organisatoriske tiltak i praksis har vært ivaretatt, skyldes at aktørene har tatt et ansvar de formelt sett ikke har.

Løsningen er kompleks og krever tilpasset opplæring for å sikre riktig bruk. Dersom tekniske tiltak ikke kan virke etter hensikten uten gode organisatoriske tiltak – for eksempel god opplæring i hvordan de tekniske tiltakene kan brukes – må dataansvaret omfatte etablering av slike organisatoriske tiltak.

Vi oppfatter at tilsynene vi har gjennomført illustrerer at håndtering av dataansvaret er krevende i en kompleks samarbeidskonstruksjon som Løsningen utgjør.

Videre er ansvars- og beslutningsstrukturen for Løsningen komplisert. Datatilsynet har brukt mye tid på å forstå hvilke beslutninger som tilligger hvilke ledd i strukturen.

Vi mener å ha fått bekreftet at helseforetakene har opplevd det som krevende å nå gjennom i beslutningsstrukturen. Etter vårt syn, har det at Helse Midt RHF representerte helseforetakene i styringsgruppen frem til november 2023 vært sterkt medvirkende i den sammenhengen. Det at helseforetakene nå er representert direkte må betegnes som en klar forbedring.

Oppsummert mener vi at ansvarsforholdene har vært uklare i praksis, selv om HP AS har vært tillagt det fulle dataansvaret for både tekniske og organisatoriske tiltak. HP AS har fremdeles det fulle dataansvaret.

Det er derfor HP AS som må holdes ansvarlig for å etablere tilstrekkelige og fungerende tiltak.

4.2 Styringssystem – rapportens punkt 6

I punkt 6.3 i tilsynsrapporten fremkommer det at HP AS ikke har etterlevd kravene til å etablere egnet systematikk for å sikre og påvise at deres behandling av personopplysninger utføres i samsvar med personvernregelverket, slik de fremgår av personvernforordningen artikkel 24, jf. artikkel 32, jf. også pasientjournalloven § 23:

- Aktørene får varierende grad av opplæring, og HP AS gir ingen bistand til utarbeidelse av egnede rutiner.
- Informasjonen til aktørene var lite strukturert og vanskelig søkbar. Informasjonen som ligger i kildene inneholder ikke styrende/kontrollerende instrukser eller rutiner som gir den dataansvarlige noen reell eller praktisk mulighet til å kontrollere etterlevelse.

Vi mener at lovbruddet er verifisert gjennom tilsynet med St. Olav, se punkt 5 og 6 i rapporten fra dette tilsynet:

- St. Olav opplevde det som krevende å få god nok informasjon fra HP AS til å gjøre vurderinger i tråd med eget dataansvar. St. Olav har utarbeidet en egen opplæringsplan og kurskatalog på til sammen flere hundre sider.

Etter vårt syn, er det nødvendig at HP AS utreder nærmere hvordan ansvaret for og oppgavene med å ivareta de organisatoriske tiltakene skal håndteres.

4.3 Tilgangsstyring, logging og loggkontroll – rapportens punkt 8

4.3.1 Revisjon og avslutning av tilganger – rapportens punkt 8.2.2.5

4.3.2 Arbeidslister – rapportens punkt 9.3

4.3.3 Manglende begrunnelse for enkeltoppslag – rapportens punkt 9.5

Under tilsynet fremkom det at sluttbrukere kan «knuse glasset» og selvautorisere seg uten å oppgi begrunnelse for oppslaget, utenom i ett tilfelle (opplysningsplikt). Dette utgjør et brudd på kravene til personopplysningssikkerhet i personvernforordningen artikkel 32, jf. også pasientjournalloven § 22.

Dette er verifisert gjennom tilsynene med St. Olav og Melhus, se rapportenes punkt 8.5.

Vi ser det nødvendig å pålegge HP AS å etablere teknisk funksjonalitet for krav til begrunnelse for følgende kategorier:

- Egen læring
- Til annen pasient
- Forskning
- Undervisning
- Innsyn
- Retting/sletting
- Pas.Admin.
- IT-relatert

HP AS må lage en tidsplan for arbeidet.

4.4 Avvikshåndtering – rapportens punkt 7

4.4.1 Avvikshåndtering generelt

HP AS har ikke iverksatt organisatoriske tiltak for å ivareta kravene til avvikshåndtering. Dette er et brudd på personvernforordningen artikkel 24, jf. artikkel 32 og 33, jf. også pasientjournalloven §§ 22 og 23.

I dialog med HP AS i etterkant av tilsynet, har det fremkommet at HP AS har videreutviklet systemet for avvikshåndtering internt. Vi ber om en redegjørelse for dette arbeidet, inkludert en beskrivelse av gjeldende system for avvikshåndtering.

Når det gjelder avvik som grunnlag for læring, fant vi også mangler ettersom HP AS ikke har gjort tilstrekkelige tiltak for å rette gjentakende og langvarige avvik som har oppstått. Dette innebærer et brudd på kravene i personvernforordningen artikkel 32, jf. artikkel 24, jf. også pasientjournalloven §§ 22 og 23.

Datatilsynet ser behov for å følge opp enkelte av disse avvikene.

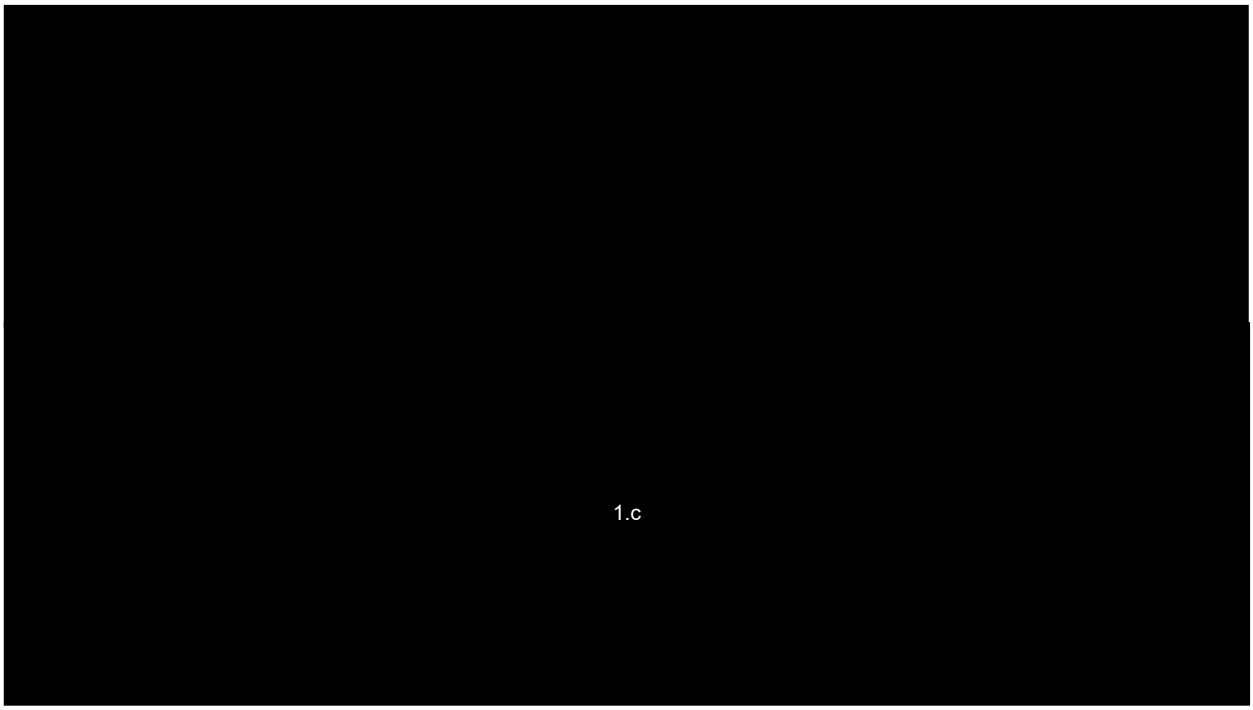
4.4.2 Arbeidslister

Manglene knyttet til arbeidslister er gjennomgått i punkt 4.3.2 foran og gjentas ikke her.

4.4.3 Helsepersonell som er inne i journal samtidig

Dette forholdet har ikke vært del av Datatilsynets tilsyn, men er kjent for oss fra Statens helsetilsyn og Statsforvalteren i Trøndelags tilsyn med St. Olav[i].

Personvernforordningen artikkel 32 nr. 1 bokstav b, jf. pasientjournalloven § 22, stiller krav om tilgjengelighet.



5. Videre saksgang

Dette er et forhåndsvarsel om vedtak, jf. forvaltningsloven § 16. Dere har rett til å uttale dere i saken før vi fatter et endelig vedtak.

Dersom dere har kommentarer til varselet om vedtak, ber vi om at disse sendes oss **innen 6. januar 2026**. Innen samme frist kan dere også anslå når en tiltaksplan/tidsplan kan foreligge.

6. Innsyn og offentlighet

Vi vil informere dere om at alle dokumentene i saken i utgangspunktet er offentlige, jf. offentlighetsloven § 3. Datatilsynet har likevel taushetsplikt om alle sikkerhetstiltak etter personvernforordningen artikkel 32, jf. personopplysningsloven § 24 første ledd andre punktum.

Med vennlig hilsen

Camilla Nervik
seksjonssjef

Susanne Lie
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Vedlegg: Endelig tilsynsrapport - Helseplattformen AS
Endelig tilsynsrapport - St. Olavs hospital HF - Helseplattformen
Endelig tilsynsrapport - Melhus kommune - Helseplattformen

[i] Se endelig tilsynsrapport punkt 5.4.1. Samtidighetskonflikt