Datatilsynet

Endelig tilsynsrapport		
Saksnummer: 24/03395 Dato for kontroll: 23.10.2024 Rapportdato: 28.11.2025	Kontrollobjekt: Melhus kommune Sted: Melhus rådhus	Utarbeidet av: Susanne Lie Fredrik Christensen

1. Innledning

Med hjemmel i personvernforordningen artikkel 57 og 58, jf. personopplysningsloven § 20, jf. pasientjournalloven § 26, gjennomførte Datatilsynet den 23. oktober 2024 et stedlig tilsyn med Melhus kommune (heretter Melhus eller kommunen).

Tilsynet var begrenset til Melhus' bruk av journalsystemet Helseplattformen.

Informasjonen vi mottok i forkant av og under tilsynet, i tillegg til dokumenter det ble avtalt under tilsynet å ettersende, danner grunnlaget for tilsynsrapporten.

2. Bakgrunn og formål med tilsynet

Journal- og samhandlingssystemet Helseplattformen (heretter Løsningen) er et felles journalsystem for helseforetak og kommunehelsetjenester i region Midt-Norge. Systemet er levert av EPIC. Helseplattformen AS (heretter HP AS) er dataansvarlig for både tekniske og organisatoriske tiltak tilknyttet Løsningen.

Løsningen som system har et stort nedslagsfelt. Det inneholder helseopplysninger og dekker et stort geografisk område, omfatter et stort antall pasienter og har et høyt antall sluttbrukere av systemet.

Etter at systemet ble satt i produksjon, har Datatilsynet mottatt et betydelig antall meldinger om brudd på personopplysningssikkerheten (avviksmeldinger) fra HP AS. I tillegg har vi mottatt bekymringsmeldinger direkte fra sluttbrukere hos aktørene som bruker systemet.

Basert på informasjon vi har mottatt gjennom avviksmeldinger, fant vi det hensiktsmessig å gjennomføre stedlig tilsyn for å kontrollere etterlevelse av kravene i personvernregelverket på utvalgte områder.

Vi gjennomførte et stedlig tilsyn hos HP AS 22. – 23. mai 2024. Som ledd i oppfølgingen av dette tilsynet, ville vi føre tilsvarende tilsyn hos et helseforetak og en kommune. Melhus ble valgt ettersom kommunen relativt nylig hadde tatt Løsningen i bruk.

Vi hadde som formål undersøke skjæringspunktet mellom HP AS' og Melhus' dataansvar, særlig knyttet til organisatoriske tiltak. Vi ville undersøke Melhus' systematikk for styring av arbeidet med personvern og personopplysningssikkerhet. Vi ønsket å se særskilt på om det er etablert et tilfredsstillende systematisk arbeid med tilgangsstyring. Videre ville vi undersøke løsningen for avvikshåndtering og -oppfølging.

3. Til stede under tilsynet

Fra Datatilsynet deltok følgende:

- Fredrik Christensen, seniorrådgiver/teknolog (tilsynsleder)
- Susanne Lie, juridisk fagdirektør
- Anders Sæve Obrestad, juridisk seniorrådgiver (observatør)

Fra Melhus deltok følgende:

- Katrine Lereggen, rådmann
- Albert Verhagen, kommunalsjef
- Geir Wormdal, IT-sjef
- Kjell Hjertås, IT-sikkerhetsansvarlig
- Phillipp Anders, systemkoordinator/lokal innføringsleder
- Stine Visnesbakk, systemkoordinator/rådgiver
- Hilde Martinsen, systemkoordinator/sluttbruker
- Runa Nesje, personvernombud

4. Kort om Helseplattformen

HP AS eies i fellesskap av helseforetakene i Helse Midt-Norge RHF og kommunene som bruker Løsningen (60/40). Den enkelte kommune er representert i beslutningsstrukturen for Løsningen.

Løsningen har ca. 45 – 50 000 unike brukere, og nedslagsfeltet omfatter ca. 750 000 pasienter som hører til den geografiske rekkevidden.

Melhus tok Løsningen i bruk i april 2024.

5. Ansvarsforhold

5.1 Relevante rettsregler

5.1.1 Dataansvaret (behandlingsansvaret) etter personvernforordningen

Plikten til å sikre etterlevelse av personvernregelverket retter seg mot den dataansvarlige. Ansvarlighetsprinsippet, som fremgår av personvernforordningen artikkel 5 nr. 2, står sterkt og stiller omfattende krav til blant annet oversiktlige rammer for behandlingen av personopplysninger.

Personvernforordningen artikkel 24 retter seg mot den dataansvarlige og pålegger virksomheten å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med forordningen. I den forbindelse, skal det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, jf. artikkel 24 nr. 1.

Den dataansvarlige har stor frihet til å delegere oppgaver og praktisk ansvar for å ivareta kravene i personvernforordningen. For å ivareta dataansvaret, forutsetter slik delegering at man har klare beskrivelser av roller, ansvar og oppgaver.

5.1.2 Dataansvaret etter pasientjournalloven

Den dataansvarliges plikter knyttet til behandlingsrettede helseregistre er regulert i pasientjournalloven § 23 om internkontroll, jf. § 22 om informasjonssikkerhet.

I pasientjournalloven § 23 er det vist til den dataansvarliges plikter etter personvernforordningen artikkel 24, jf. det som er sagt om denne bestemmelsen over.

5.1.3 Vedtaket om dataansvar etter pasientjournalloven § 9

Pasientjournalloven § 9 regulerer situasjonen der to eller flere virksomheter samarbeider om behandlingsrettede helseregistre. Virksomhetene skal da inngå skriftlig avtale om blant annet dataansvar, jf. § 9 bokstav d. I bestemmelsens annet ledd fremgår det at departementet kan sette vilkår for samarbeidet gjennom forskrift eller enkeltvedtak.

I vedtak av 22. mars 2022 har Helse- og omsorgsdepartementet (HOD) besluttet fordelingen av dataansvaret mellom HP AS og aktørene.

På side 3 i vedtaket fremgår det at «[v]edtaket fastsetter dataansvaret ved å fordele oppgaver mellom helsevirksomhetene og Helseplattformen AS. Dataansvaret til Helseplattformen AS er avgrenset mot oppgaver knyttet til helsefaglige vurderinger. Dataansvaret er uttømmende definert i enkeltvedtaket. En nærmere tydeliggjøring av forpliktelser og oppgaver/aktiviteter for å oppfylle dataansvaret spesifiseres i den tjenesteavtalen som vil inngås mellom Helseplattformen AS og den enkelte virksomhet for bruk av Helseplattformen».

Videre fremgår det i punkt 2.1 om ansvaret for informasjonssikkerhet:

> «Helseplattformen AS har det overordnede ansvaret for informasjonssikkerheten i Helseplattformen. I dette ligger et ansvar for å gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Tiltakene skal motvirke utilsiktet eller ulovlig tilintetgjøring, tap, endring

eller ikke-autorisert utlevering av eller tilgang til helse- og personopplysninger som er overført, lagret eller på annen måte behandlet i Helseplattformen, jf. pasientjournalloven § 22».

5.2 Faktiske forhold

5.2.1 Innhold i og regulering av dataansvaret

Grensegangen mellom HP AS' og aktørenes dataansvar er overordnet beskrevet i vedtaket fra HOD datert 22. mars 2022. Der fremgår det at HP AS' dataansvar er avgrenset mot helsefaglige vurderinger, som skal gjøres av den enkelte aktør. HP AS har ansvar for informasjonssikkerheten i løsningen, både for tekniske og organisatoriske tiltak. Eventuell oppgavefordeling klarlegges i Tjenesteavtalen.

5.2.2 HP AS' organisatoriske tiltak overfor aktørene

I Tjenesteavtalen punkt 3.2 er det beskrevet et planverk for etableringsfasen. Det fremgår at HP AS skal styre gjennomføring av etableringsfasen (innføring) gjennom a) prosjektplan, b) aktivitetsplan, c) testplan og d) opplæringsplan.

Prosjektplanen skisserer hvilke hovedaktiviteter som må gjennomføres og milepælene som skal oppnås frem til innføring. Aktivitetsplanen tar utgangspunkt i prosjektplanen og er tilpasset kundespesifikke behov. Testplanen er aktørspesifikk og skal sikre relevant testing av lokale tilpasninger. Opplæringsplanen innebærer at HP AS skal lære opp særskilte ressurser hos aktørene, etter «train the trainer»-prinsippet. Det fremgår at aktørene må etablere en egen plan for opplæring internt.

Organisatoriske tiltak er for øvrig ikke beskrevet i Tjenesteavtalen.

5.2.3 Kommunens organisatoriske tiltak

Under tilsynet stilte Datatilsynet spørsmål om hvordan HP AS i forbindelse med innføring satt Melhus i stand til å bruke Løsningen på en trygg og riktig måte.

Melhus beskrev at HP AS la frem en kravspesifikasjon med ansvarsfordeling og hva Melhus måtte ha på plass før iverksettelse av Løsningen. Videre fremkom det at Tjenesteavtalen er konkretisert gjennom et rollekart, der kommunen har definert hva som er dens rolle. HP AS har anbefalt roller i kommunal forvaltning i rollekartet, og Melhus har lagt rollene til ansatte med rett kompetanse.

Melhus opplyste at de tidlig mottok kommunikasjonsmateriell fra HP AS, som kommunen tilpasset etter egne behov for å synliggjøre at kommunen hadde eierskap til prosessen.

Videre beskrev Melhus at kommunen har fulgt HP AS' opplæringsopplegg «fra a til å», med instruktøropplæring, superbrukeropplæring, systemlæring gjennom klasseromskurs og egentrening gjennom e-læring. Katalogen for e-læring ble beskrevet som bra.

Kommunen har hatt en stor rigg for superbrukere, med ca. 20 % dekning blant de ansatte. Melhus har fulgt EPICs anbefalinger om antall superbrukere.

HP AS har også laget pakker for ulike fagområder, som opplevdes som nyttige av de ansatte.

5.3 Datatilsynets vurdering og konklusjon

Det fremgår av vedtaket fra HOD av 22. mars 2022 at HP AS som dataansvarlig har ansvar for både tekniske og organisatoriske tiltak. Vår erfaring er at HP AS fullt ut har påtatt seg ansvaret for de tekniske funksjonalitetene i Løsningen, enten disse er besluttet i beslutningsstrukturen eller tilligger HP AS' eget ansvar. For de organisatoriske tiltakene har det imidlertid vært mer uklart hvordan ansvar og oppgaver er fordelt.

Under tilsynet fremkom det at Melhus opplevde opplæringsmateriellet som HP AS har tilbudt som dekkende og godt. Kommunen har ikke sett behov for å utarbeide egen veiledning eller opplæring til de ansatte.

De organisatoriske tiltakene vi har vurdert under tilsynet mot Melhus oppfyller i praksis kravene i personvernforordningen artikkel 24, jf. pasientjournalloven § 23.

6. Styringssystem

6.1 Rettslig grunnlag

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

Ansvaret innebærer en forpliktelse til å gjennomføre egnede tekniske og organisatoriske tiltak jf. personvernforordningen artikkel 24. Tiltakene skal gjennomgås og oppdateres ved behov, jf. artikkel 24 nr. 1 siste setning og artikkel 32 nr. 1 bokstav d. Personvernforordningen forplikter den ansvarlige til å iverksette retningslinjer dersom det står i et rimelig forhold til behandlingsaktivitetene, jf. artikkel 24 nr. 2.

Pasientjournalloven § 23 oppstiller også tilsvarende krav, og bestemmelsen viser til personvernforordningen artikkel 24.

Pasientjournalloven presiserer at den dataansvarlige skal dokumentere tiltakene og at dokumentasjonen skal være tilgjengelig for medarbeiderne hos den dataansvarlige. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.

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

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

Personvernregelverket angir at det skal gjøres konkrete vurderinger knyttet til hva som kreves av organisatoriske tiltak i form av et styringssystem, ettersom det «skal stå i et rimelig forhold til behandlingsaktivitetene». Det er opp til den dataansvarlige å sikre at systemet er egnet til å oppfylle hensikten innenfor den aktuelle virksomheten.

Helseopplysninger er en særlig kategori av personopplysninger, og det stilles derfor strenge krav til styringen av pasientjournalsystemer. Kravene i personvernregelverket er blant annet operasjonalisert i Normen for informasjonssikkerhet og personvern i helse- og omsorgstjenesten. Nasjonal sikkerhetsmyndighets grunnprinsipper kan også gi god veiledning om hvordan kravene skal ivaretas i praksis.

6.2 Faktiske forhold

6.2.1 Innsendt dokumentasjon

I forkant av tilsynet oversendte Melhus dokumentasjon i tråd med vårt pålegg i varsel om tilsyn datert 12. september 2024.

6.2.2 Styringssystemet EQS

Melhus har etablert sitt styringssystem i verktøyet Extended Quality System (EQS), som er et modulbasert kvalitetssystem for kvalitets- og virksomhetsstyring. EQS er konfigurert og tilpasses etter som hvilken rolle som benytter systemet.

Melhus redegjorde for at EQS bygger på ISO-rammeverk, NIS2 og NSMs grunnprinsipper. Som et utgangspunkt har kommunen også sett hen til KiNS' eksempel på styringssystem.

Det fremkom av demonstrasjonen av EQS at styringssystemet er satt opp på en oversiktlig måte for sluttbrukere. EQS inneholder blant annet en egen mappe som heter «Helseplattformen overordnet», med overordnede retningslinjer for tilgangsstyring, avviksbehandling mv. Melhus beskrev et pågående arbeid for å innlemme alle kommunens eksisterende rutiner i EQS.

Revisjon av innholdet er styrt per dokument. Hvert enkelt dokument eller område er satt opp med en dokumentansvarlig og en dokumenteier. Revisjonsfrister varsles på e-post. Disse går først til dokumentansvarlig, deretter til dokumenteier om revisjonsfristen ikke er overholdt.

6.3 Datatilsynets vurdering og konklusjon

En velfungerende og sterk styringssystematikk for organisatoriske og tekniske tiltak anses som et nødvendig verktøy for at den dataansvarlige skal kunne sikre og påvise at personvernregelverket er ivaretatt. Løsningens organisering og struktur nødvendiggjør et omfattende styringssystem.

I vurderingen av hva et styringssystem må inneholde, skal det tas hensyn til personopplysningene som behandles i Løsningen. Tatt i betraktning at Løsningen inneholder opplysninger om et stort antall pasienter, og at systemet er bygget for samhandlingsformål, stilles det strenge krav til hvilke organisatoriske tiltak den dataansvarlige skal etablere.

Etter vår vurdering, har Melhus et fungerende og enkelt tilgjengelig styringssystem i EQS. Systemet anses som egnet for formålet. Selv om systemet innholdsmessig ikke var komplett på tidspunktet for tilsynet, vurderes innholdet og oppsettet som godt nok for temaene som tilsynet gjelder.

Datatilsynet vurderer at styringssystemet som Melhus har etablert lokalt i praksis dekker behovene kommunen har, jf. personvernforordningen artikkel 24, jf. artikkel 32, jf. også pasientjournalloven § 23.

7. Tilgangsstyring, logging og loggkontroll

7.1 Relevante rettsregler

7.1.1 Personvernforordningen

De grunnleggende kravene til personopplysningssikkerhet fremkommer i personvernforordningen artikkel 32 nr. 1, som stadfester at den behandlingsansvarlige må gjennomføre «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen» ved behandlingen av personopplysninger.

Bestemmelsen gir anvisning på en risikobasert og skjønnsmessig tilnærming. Hensikten er at sikkerhetstiltakene skal stå i et rimelig forhold til den konkrete risikoen ved behandlingen. Dette forutsetter at den behandlingsansvarlige gjennomfører risikovurderinger, hvilket også er et krav etter artikkel 32 nr. 2.

I pasientjournalsystemer er det på det rene at tilgangsstyring er et nødvendig element i tiltakene som er påkrevd etter personvernforordningen artikkel 32. Bestemmelsens bokstav b stiller krav om at den dataansvarlige har etablert tiltak som gir «evne til å sikre vedvarende konfidensialitet» hvor risikovurderingen tilsier at det er nødvendig. Bokstav d stiller krav om at den dataansvarlige etablerer «en prosess for regelmessig testing, analysering og vurdering av hvor effektive» de øvrige sikkerhetstiltakene er.

Summen av tiltak knyttet til tilgangsstyring, logging og loggkontroll avgjør om konfidensialitetsnivået er tilfredsstillende. Dette innebærer at loggkontrollen til en viss grad kan tilpasses valgt nivå av tilgangsstyring. Vide tilganger tilsier en streng loggkontroll. Omvendt kan en streng og snever tilgangsstyring tilsi et mindre behov for å kontrollere logger. Tekniske tiltak må suppleres med organisatoriske tiltak, som opplæring og rutiner. Dette krever et egnet styringssystem. Kvaliteten på styringssystemet har derfor innvirkning på hvorvidt sikkerhetstiltakene anses tilfredsstillende.

Prinsippet kalt «tjenstlig behov», som blant annet kommer til uttrykk gjennom regler om taushetsplikt og nødvendighetskriteriet i dataminimeringsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav c, står sentralt i den sammenhengen. Ansatte skal kun ha tilgang til opplysninger som er relevante og nødvendige for arbeidet deres.

7.1.2 Pasientjournalloven og pasientjournalforskriften

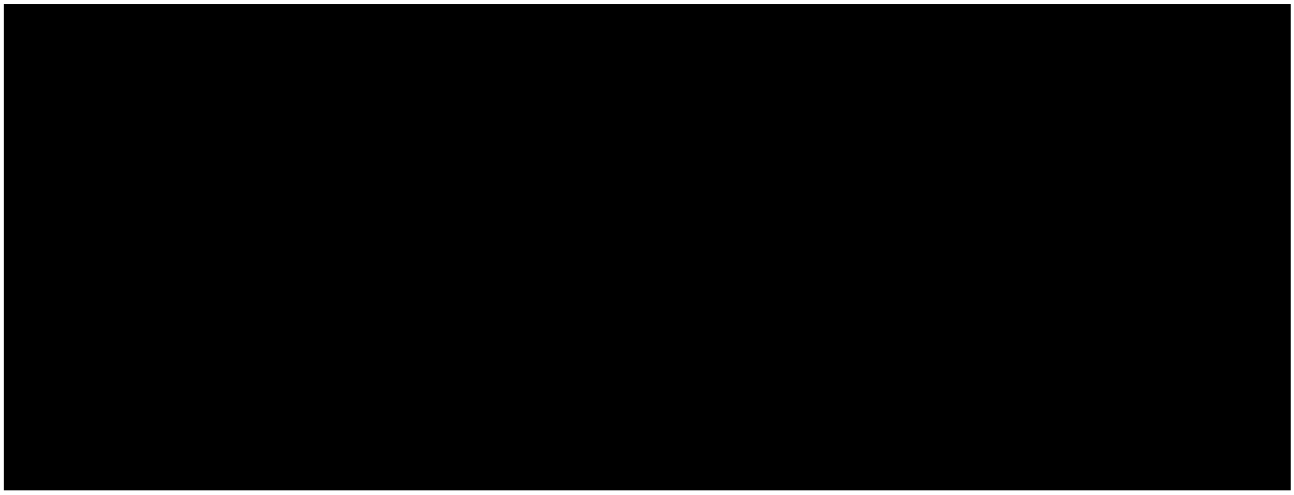
Pasientjournalloven § 22 forplikter den dataansvarlige og databehandleren til å gjennomføre tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå. Bestemmelsen viser til personvernforordningen artikkel 32. I § 22 første ledd annet punktum presiseres det at den dataansvarlige blant annet skal sørge for tilgangsstyring, logging og etterfølgende kontroll.

Pasientjournalforskriften § 13 stiller nærmere krav til tilgangsstyring av journalopplysninger. Det stilles blant annet krav til autorisasjon, oversikt over tildelte tilganger, tidsbegrensninger av tilganger og revisjonsaktiviteter. Bestemmelsen slår fast den dataansvarliges plikt til å ha oversikt over hvem som har tilgang til hvilke typer opplysninger og evne til å kontrollere faktisk bruk.

Pasientjournalforskriften § 14 regulerer oppstiller nærmere krav om loggføring og slår fast at tilgjengeliggjøring av opplysninger skal registreres automatisk, med nærmere spesifikasjoner av hva registreringen (loggen) skal inneholde.

7.2 Faktiske forhold

7.2.1 Tildeling, revisjon og avslutning av tilganger



[redacted]

Datatilsynets vurdering og konklusjon

Vi legger til grunn at Melhus bruker eksisterende funksjonalitet for tilgangsstyring i Løsningen og at denne i all hovedsak dekker kommunens behov.

Vi har kommet til at Melhus har etablert gode organisatoriske tiltak for å ivareta tildeling, revisjon og avslutning av tilganger ved kommunens bruk av Løsningen. Melhus oppfyller dermed i praksis kravene i personvernforordningen artikkel 32, jf. artikkel 24, jf. også pasientjournalloven §§ 22 og 23, ved den lokale bruken av Løsningen.

[redacted]

7.2.2 Lokale tilpasninger

Under tilsynet stilte Datatilsynet spørsmål om hvorvidt det var mulighet for å tilpasse innholdet i tilgangsrollene ut fra lokale forhold.

[redacted]

[redacted]

Datatilsynets vurdering og konklusjon

Vi legger til grunn at Melhus benytter seg av tilgjengelig funksjonalitet for tilgangsstyring i Løsningen og at denne i all hovedsak er tilpasset kommunens behov.

Vi har kommet til at Melhus har etablert gode organisatoriske tiltak for tilgangsstyring ved helseforetakets bruk av Løsningen. Melhus oppfyller dermed i praksis kravene som følger av personvernforordningen artikkel 32, jf. artikkel 24 og pasientjournalloven § 22, ved den lokale bruken av Løsningen.

8. Konkrete funksjonaliteter

8.1 Relevante rettsregler

Vi viser her til punkt 7.1.1 og 7.1.2.

8.2 Arbeidsflate

Med «arbeidsflate» mener vi første visningsbilde ved pålogging på brukerkonto. Under tilsynet demonstrerte Melhus arbeidsflaten i Løsningen.

Melhus beskrev at arbeidsflaten varierer ut fra hvilken enhet i kommunen den ansatte er tilknyttet. Kommunen anga at deres ansatte opplever informasjonen som relevant.

Første visningsbilde gir en oversikt med generell informasjon når en pasient/bruker er klikket på én gang. Det ble likevel bemerket at det ikke nødvendigvis er relevant eller nødvendig å få opplysninger om pasientens/brukerens neste sykehustime. Melhus har diskutert dette internt og hvorvidt det skal bes om endring.

Videre beskrev Melhus at et «storyboard» vises på venstre side av visningsbilde når ansatte er inne i journal. Her vises nyttig informasjon som det kan være relevant for behandlende personell å ha enkel tilgang til.

I arbeidsflaten er det også et menyvalg for Kunnskapsbasen, som er mye brukt av deres ansatte og oppleves som et nyttig verktøy. Kunnskapsbasen har klinisk brukerveiledning, men man kan også benytte basen for bestilling av rapporter for administrative behov.

Datatilsynets vurdering og konklusjon

Vi legger til grunn at informasjonen som fremkommer i ansattes arbeidsflate i all hovedsak er vurdert som nødvendig og relevant av kommunen.

Vi har ikke avdekket informasjon som tilsier at kravet til konfidensialitet som følger av personvernforordningen artikkel 32, jf. også pasientjournalloven § 22, er brutt gjennom Melhus' bruk av eksisterende funksjonalitet for arbeidsflatevisning.

8.3 Arbeidslister

Funksjonen arbeidslister har vært tema i mange av avviksmeldingene til Datatilsynet. Melhus kaller arbeidslister for «timeplan».

Under tilsynet demonstrerte Melhus hvordan en arbeidsliste ser ut for en klinisk sluttbruker. Sluttbrukeren får en «timeplan», som er en liste over alle pasienter den ansatte er tildelt den dagen. Når man trykker på en pasient en gang, får man en oversikt med generell informasjon, herunder siste 20 besøk og gjøremål for besøket. I tillegg får man oversikt over besøk for de kommende syv dagene.

Datatilsynets vurdering og konklusjon

Datatilsynet legger til grunn at Melhus har benyttet seg av funksjonaliteten som har vært tilgjengelig i Løsningen og innrettet sin virksomhet i tråd med dette.

Det kan stilles spørsmål ved om alle ansatte har behov for funksjonaliteten arbeidslister. Vi har imidlertid ikke grunnlag for å si at behovet ikke er til stede.

Vi har kommet til at det ikke er grunnlag for å konkludere med at Melhus har brutt kravet til konfidensialitet som fremgår i personvernforordningen artikkel 32 gjennom sin bruk av Løsningen, jf. artikkel 24, jf. også pasientjournalloven §§ 22 og 23.

8.4 Pasientsøk

Under tilsynet fremkom det at alle ansatte har tilgang til funksjonen Pasientsøk. Melhus har egen rutine for Pasientsøk, som ble fremvist under tilsynet.

Melhus forklarte at funksjonaliteten er relevant for alle deres ansatte, da de kan måtte legge til nye brukere/pasienter. Administrativt må ansatte kunne søke opp pasienter. Videre beskrev kommunen at ansatte kan måtte reise ut på alarmer, og da er det essensielt å kunne finne riktig pasient uten en gitt arbeidsliste eller rolle/mal som er knyttet til en behandlingsrelasjon.

Pasientene som kan søkes opp gjennom Pasientsøk er avgrenset til egne kommunale pasienter/brukere.

[redacted]

Datatilsynets vurdering og konklusjon

Vi tar til etterretning at Melhus har vurdert det som hensiktsmessig at alle ansatte har tilgang til Pasientsøk, da mange ulike personellgrupper har behov for funksjonen. Kommunen har rutiner for Pasientsøk, og det er mulig å føre loggkontroll med funksjonaliteten.

Vi har kommet til at Melhus legger til rette for tilstrekkelig tilgangsstyring for funksjonaliteten Pasientsøk gjennom sin bruk av Løsningen, i tråd med kravene i personvernforordningen artikkel 32, jf. også pasientjournalloven § 22.

8.5 «Knus glasset»-funksjonen

Datatilsynet ønsket å undersøke kommunens bruk av funksjonaliteten «knus glasset». Formålet med funksjonen er å tilgjengeliggjøre pasientjournal for helsepersonell når systemet ikke gjenkjenner en behandlingsrelasjon mellom helsepersonell og pasient.

Melhus opplyste at alle deres ansatte har tilgang til «knus glasset»-funksjonen, men at funksjonskode vil avgjøre hvilken gradering av «knus glasset» den ansatte får tilgang til.

Kommunen anga at nesten all bruk av «knus glasset»-funksjonen i deres virksomhet gjøres med begrunnelsesvalg «Helsehjelp». Ettersom det ikke er påtvunget å skrive en begrunnelse for tilgang, har kommunen lært opp ansatte i at dette likevel bør gjøres. Kommunen skulle gjerne sett at skriftlig begrunnelse ved bruk av «knus glasset»-funksjonen var påkrevd i Løsningen, slik at de har god sporbarhet knyttet til om det har vært tjenstlig behov for det enkelte oppslag.

Datatilsynets vurdering og konklusjon

Vi legger til grunn at «knus glasset»-funksjonen er innrettet og brukes på en måte som dekker Melhus' behov. Kommunen fører også god kontroll med funksjonaliteten.

Vi har kommet at Melhus har etablert gode lokale tiltak for å sikre at bruken av Løsningen er i tråd med kravene til personopplysningssikkerhet i personvernforordningen artikkel 32, jf. også pasientjournalloven § 22.

Datatilsynet har merket seg mangelen på krav til begrunnelse for enkeltoppslag. Dette er imidlertid et teknisk spørsmål som faller utenfor Melhus' dataansvar.

8.6 Særlig beskyttelsesverdige opplysninger

8.6.1 Fortrolig/strengt fortrolig adresse

Under tilsynet fremviste Melhus sin egen omfattende rutine i EQS for hvordan kommunen behandler informasjon om beskyttelsesverdige pasienter. Rutinen bygger på tilsvarende rutiner hos Trondheim kommune og St. Olav hospital HF.

Datatilsynets vurdering og konklusjon

Melhus har en egen rutine som gjelder skjerming av pasienter med fortrolig/strengt fortrolig adresse. Etter rutinen er det tydelige avgrenset hvilke ansatte som får se opplysninger om pasienter/brukere med fortrolig/strengt fortrolig adresse.

Vi har kommet til at Melhus har etablert gode organisatoriske tiltak lokalt for skjerming av egne pasienter med fortrolig/strengt fortrolig adresse i tråd med kravene til konfidensialitet, jf. personvernforordningen artikkel 32, jf. artikkel 24, jf. også pasientjournalloven §§ 22 og 23.

8.6.2 Kommunens egne ansatte

Under tilsynet etterspurte Datatilsynet hvordan kommunens egne ansatte ivaretas når de er pasient på egen arbeidsplass.

Melhus fortalte at de har rutine for skjerming av egne ansatte i Løsningen. Det finnes teknisk funksjonalitet for dette. Kommunen påpekte også at man kan skjerme pasienter for spesifikke ansatte.

Datatilsynets vurdering og konklusjon

Vi har kommet til at Melhus har etablert egnede tiltak lokalt for å skjerme egne ansatte i tråd med kravene til konfidensialitet i personvernforordningen artikkel 32, jf. også pasientjournalloven § 22.

8.6.3 Særskilte pasientgrupper

Under tilsynet spurte Datatilsynet om hvordan opplysninger knyttet til særskilte pasientgrupper blir ivaretatt i Løsningen.

Melhus opplyste at de har en egen brukerveiledning om dette i EQS. [redacted]

Datatilsynets vurdering og konklusjon

Vi har kommet til at Melhus har etablert egnede organisatoriske tiltak lokalt for skjerming av journal for egne særskilte pasientgrupper i tråd med kravene i personvernforordningen artikkel 32, jf. også pasientjournalloven § 22.

8.6.4 Pasienter i offentlig søkelys mv.

Under tilsynet undersøkte Datatilsynet om Melhus bruker funksjonalitet for å skjerme enkeltpasienter som er i offentlig søkelys («kjendiser»), pasienter av nyhetsinteresse e.l.

Melhus opplyste at de ikke er kjent med spesiell funksjonalitet for dette, og det har heller ikke kommet opp tilfeller hvor dette ville blitt brukt. Kommunen anga at ordinær rutine og funksjonalitet for skjerming av pasient ville vært gjeldende.

Datatilsynets vurdering og konklusjon

Datatilsynet vurderer at Melhus har etablert tilstrekkelige organisatoriske tiltak lokalt for skjerming av journal for enkeltpersoner som er i offentlig søkelys eller av nyhetsinteressesom i praksis oppfyller kravene i personvernforordningen artikkel 32, jf. artikkel 24, jf. også pasientjournalloven §§ 22 og 23.

8.6.5 Pasientsperrede journaler

Under tilsynet opplyste Melhus at pasienter selv kan sperre innsyn i journal gjennom pasientapplikasjonen HelsaMi. [redacted]

Datatilsynets vurdering og konklusjon

Vi legger til grunn at Melhus har funksjonalitet tilgjengelig for pasientinitiert sperring av journal. Selv om kommunen har rom for forbedring av rutinene, har vi kommet til at Melhus har etablert tilstrekkelige organisatoriske tiltak lokalt for skjerming av journal der pasienter ber om det som i praksis oppfyller kravene i personvernforordningen artikkel 32, jf. også pasientjournalloven § 22.

9. Avvikshåndtering

9.1 Relevante rettsregler

9.1.1 Personvernforordningen

Den dataansvarlige har ansvar for å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen av personopplysninger utføres i samsvar med personvernforordningen, jf. personvernforordningen artikkel 24. Tiltakene skal gjennomgås regelmessig og skal oppdateres ved behov.

Den dataansvarlige plikter å dokumentere ethvert brudd på personopplysningssikkerheten, herunder hendelsesforløpet, konsekvensene og tiltakene som er truffet for å utbedre svikten, jf. personvernforordningen artikkel 33 nr. 5.

Dersom det skjer et brudd på personopplysningssikkerheten, også kalt avvik, har den dataansvarlige som hovedregel plikt til å melde det til Datatilsynet innen 72 timer, jf. artikkel 33 nr. 1.

Systematisk avvikshåndtering er en naturlig del av den dataansvarliges plikt til internkontroll etter personvernforordningen artikkel 24. Håndtering og oppfølging av avvik kan gi viktig lærdom og er sentralt for å forhindre at tilsvarende sikkerhetsbrudd i fremtiden.

Resultater, tiltak, og erfaringer tilknyttet avvikshåndtering påvirker derfor også sikkerheten ved behandlingen av personopplysninger, jf. artikkel 32.

9.1.2 Pasientjournalloven

I pasientjournalloven § 23 om internkontroll, er det vist til den dataansvarliges plikter etter personvernforordningen artikkel 24, jf. det som er sagt om denne bestemmelsen over.

Videre viser pasientjournalloven § 22 om informasjonssikkerhet til kravene til personopplysningssikkerhet i personvernforordningen artikkel 32.

9.1.3 Vedtaket etter pasientjournalloven § 9

I vedtaket fra HOD av 22. mars 2022, der dataansvaret i Helseplattformen fastsettes, fremgår følgende i punkt 2.7 om brudd på personopplysningssikkerheten:

> «Dersom en helsevirksomhet identifiserer et brudd på personopplysningssikkerheten jf. pasientjournalloven § 22, jf. personvernforordningen artikkel 4 nr. 12, skal helsevirksomheten omgående varsle Helseplattformen AS. Helseplattformen AS er ansvarlig for å følge opp avviket, herunder rapportere videre til de andre helsevirksomhetene i samarbeidet, tilsynsmyndighetene og de registrerte, jf. personvernforordningen artikkel 33 og 34. Dette gjelder også dersom Helseplattformen AS selv oppdager avviket.

Helseplattformen AS [skal også] sørge for å gi helsevirksomhetene jevnlige statusoppdateringer om det enkelte avvik og gi helsevirksomhetene opplysningene som er nødvendige for å kunne følge opp disse».

9.2 Faktiske forhold

9.2.1 System for avvikshåndtering

Under tilsynet demonstrerte Melhus hvordan systemet for avviksmelding er bygget opp i EQS. Alle ansatte i Melhus kan melde avvik, og meldeskjemaet er lett tilgjengelig som menyvalg. I meldeskjemaet er det også lenket til rutinen for avviksmelding. Meldeskjemaet er bygd opp etter hvordan Datatilsynet ønsker at virksomhetene melder avvik om brudd på personopplysningssikkerheten.

Det fremkom at avvik kan meldes til forskjellige enheter. Den ansatte melder avvik til egen enhet, og nærmeste leder behandler innmeldte avvik. Leder gjør en vurdering om avviket er relatert til Løsningen. I tvilstilfeller sendes avviket til personvernombudet, som gjør en faglig vurdering. Hvis avviket er relatert til Løsningen, melder leder saken i ServiceNow som en vanlig supportsak. Leder skal også vurdere kritikaliteten av meldingen.

Kommunalsjef og systemkoordinator mottar eget varsel om avvik knyttet til Løsningen, personvern og informasjonssikkerhet. Videre mottar kommunalsjef kopi av alle helserelaterte avvik i EQS.

[redacted]

Kommunen beskrev at de opplevde rutinene for melding av avvik som tilstrekkelige og godt fungerende.

Melhus opplyste også at de er en part i det regionale informasjonssikkerhetsforumet (RIF). Der gjøres det månedlig gjennomgang av innmeldte avvik sammen med HP AS. Kommunen kan også få tilgang til liste over rapporterte avvik fra HP AS på forespørsel.

Kommunen redegjorde for at avvik regelmessig brukes i opplæring, og erfaringene ligger til grunn for oppdatering av styringssystemet. Rapportering av avvik er også en del av ledelsens årlige gjennomgang.

Datatilsynets vurdering og konklusjon

Etter vår vurdering, har Melhus etablert et egnet system for avvikshåndtering i form av EQS. Kommunen har demonstrert for Datatilsynet at operativ bruk av systemet er god og hensiktsmessig.

Vi anser også at Melhus har tilrettelagt godt for at ansatte gjøres kjent med rutinene for avviksmelding.

Vi har kommet til at Melhus har etablert et egnet system for avvikshåndtering lokalt som tilfredsstiller kravene i personvernforordningen artikkel 24, jf. artikkel 33, jf. også pasientjournalloven § 23.

9.2.2 Ansvar for avvikshåndtering, herunder meldeplikt til Datatilsynet

I enkeltvedtaket fra HOD datert 22. mars 2022, kommer det tydelig frem i punkt 2.1 at HP AS har det overordnede ansvaret for informasjonssikkerheten i Løsningen, herunder for tekniske og organisatoriske tiltak. Dette må omfatte avvikshåndtering tilknyttet Løsningen.

Videre fremgår det i punkt 2.7 at brudd på personopplysningssikkerheten skal meldes fra aktørene til HP AS og at HP AS er ansvarlig for å følge opp avvikene.

Under tilsynet opplyste Melhus at HP AS håndterer alle avvik som er knyttet til Løsningen. Melhus har meldt få avvik til HP AS siden innføring. Kommunens erfaring er at HP AS håndterte avviket raskt og at den ansatte som meldte avviket raskt fikk tilbakemelding.

Melhus beskrev at kommunikasjonen med HP AS knyttet til avvikshåndtering er god. Blant annet har Melhus mulighet til å gjenåpne meldte saker hvis kommunen ikke er enig i løsningsforslaget, eller at iverksatte tiltak ikke fungerer operativt.

Kommunen anga at informasjon om 72-timersfristen er innbakt i rutinen for avviksmeldinger.

Datatilsynets vurdering og konklusjon

Vi legger til grunn at det er klart for Melhus hvilken virksomhet (kommunen eller HP AS) som har ansvaret for å melde hvilke avvik.

Avvik innenfor feltene Løsningen og personvern//informasjonssikkerhet blir gjennomgått fortløpende. Det er likevel en viss risiko for at avvik som er feilklassifiserte av melder ikke fanges opp tidsnok til at 72-timersfristen kan overholdes. Vi mener likevel at denne risikoen ikke er betydelig nok til å konkludere med regelverksbrudd.

Vi vurderer at Melhus har et bevisst forhold til hvilke tiltak kommunen eventuelt er ansvarlig for å iverksette etter at avvikene er vurdert av HP AS.

Vi har kommet til at Melhus har etablertegnede tekniske og organisatoriske tiltak lokalt for å ivareta kravene til avvikshåndtering som fremgår av personvernforordningen artikkel 24, jf. artikkel 32 og 33, jf. også pasientjournalloven §§ 22 og 23.