

OSLO UNIVERSITETSSYKEHUS HF
Postboks 4956 Nydalen
0424 OSLO

Deres referanse

Vår referanse
20/01657-2

Dato
07.07.2020

Krav om redegjørelse - melding om avvik - Oslo Universitetssykehus HF

Datatilsynets oppgave er å føre kontroll etter personopplysningsregelverket slik at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Sakens bakgrunn

Vi viser til avviksmelding sendt til oss på e-post 18. mai 2020 og varsel til personer som har blitt eksponert på offentlig journal med navn og/eller personnummer datert 20. mai 2020, som vi mottok kopi av 22. mai 2020. I varselet opplyses det om at avviket er meldt til Datatilsynet.

Vi har forståelse for at avviket meldes trinnvis jf. personvernforordningen artikkel 33 pkt. 4 ettersom avviket omfatter et stort antall berørte, har pågått i lang tid og det kan kreve noe tid å få oversikt over årsak, konsekvenser og nødvendige tiltak. Dersom det gis trinnvis informasjon skal utfyllende informasjon gis uten ytterligere ugrunnet opphold.

Rettslig bakgrunn

Dere har plikt til å hindre uautorisert tilgang til personopplysninger hvor det er behov for konfidensialitet. Opplysninger om at en person er pasient ved sykehuset vil i mange tilfeller ikke bare være en opplysning om personlige forhold, men også en helseopplysning. Sykehusets plikt til konfidensialitet følger av helsepersonellovens §§ 21 flg. Det er også fastsatt i forskrift om offentlig journal § 10 at «opplysninger som er omfatta av teieplikt i lov eller i medhald av lov skal ikkje gå fram av den offentlege journalen».

Pasientjournalloven §§ 22 og 23 inneholder krav til informasjonssikkerhet og internkontroll som skal sikre at sykehusets behandling av personopplysninger skjer i samsvar med personvernforordningen artikkel 32 og 24.

Eventuelle brudd på informasjonssikkerheten som kan ha konsekvenser for den registrertes rettigheter og friheter skal varsles til Datatilsynet senest innen 72 timer etter at bruddet ble oppdaget jf. personvernforordningen artikkel 33. Virksomheten plikter å dokumentere ethvert personvernbrudd, herunder de faktiske forhold rundt nevnte brudd, virkningen av det og hvilke tiltak som er truffet for å utbedre det. Dokumentasjonen skal gjøre det mulig for tilsynsmyndigheten å kontrollere samsvar med artikkel 33, jf. artikkel 33 pkt. 5.

Vi ber om svar på følgende:

1. Hvilke rutiner har dere for å sikre at plikten til å melde avvik til Datatilsynet i samsvar med personvernforordningen artikkel 33 etterleves? Vi visert til personvernforordningen artikkel 33 pkt. 5 og ber om utfyllende informasjon om de faktiske forholdene rundt avviket, virkningen av det og hvilke tiltak som er truffet for å utbedre det, herunder svar på følgende spørsmål:
 - a. Hva er årsaken til at denne type avvik har pågått over en lang tidsperiode?
 - b. Hvilke kategorier av registrerte er berørt og hva slags informasjon er offentliggjort i tillegg til personnummer?
 - c. Hvilke undersøkelser er gjort for å finne ut om avviket omfatter flere tilfeller enn det som ble avdekket i varsel til sykehuset?
 - d. Hvilke konsekvenser har avviket hatt for de registrerte, eller kategorier av registrerte avhengig av hva slags informasjon som er publisert?
 - e. Hvilke tiltak er truffet eller planlagt gjennomført for å håndtere personvernbruddet, herunder tiltak for å redusere skadevirkninger som følge av bruddet og forhindre at liknende avvik gjentar seg?

2. Vi har forstått at dere ble oppmerksom på avviket som følge av et varsel fra tredjepart. Hvordan sikrer virksomheten selv at lovpålagt taushetsplikt ivaretas ved føring av offentlig journal jf. forskrift om offentlig journal § 10, slik at publisering av postjournal ikke medfører personvernbrudd? Legg ved dokumentasjon på rutiner som var gjeldende da avviket ble oppdaget.

Videre fremdrift

Dere må sende oss utfyllende informasjon om avviket inkludert svar på våre spørsmål innen **28. juli 2020**.

Hjemmelsgrunnlag

Etter personvernforordningen artikkel 58 nr. 1 har vi myndighet til å kreve de opplysningene som trengs for at vi skal kunne gjennomføre oppgavene våre.

Klageadgang

Dere kan klage på pålegget om å gi oss informasjon. En eventuell klage må sendes til oss **innen tre dager** etter at dette brevet er mottatt (jf. forvaltningsloven § 14). Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernemnda for klagebehandling.

Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3.) Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn ber vi dere om å begrunne dette.

Mer informasjon om personvern, internkontroll og informasjonssikkerhet kan dere finne på våre nettsider, www.datatilsynet.no.

Hvis dere har spørsmål, kan dere ta kontakt med Grete Alhaug på telefon 90781530.

Med vennlig hilsen

Grete Alhaug
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: OSLO UNIVERSITETSSYKEHUS HF, Tor Åsmund Martinsen