



Styre: Universitetsstyret

Styresak: 76/15

Møtedato: 27.08.2015

Dato: 18.08.2015

Arkivsaksnr: 2014/9326

Orientering om varsel om vedtak og varsel om overtredelsesgebyr fra Datatilsynet

Bakgrunn

Universitetet har fått varsel om vedtak og varsel om overtredelsesgebyr på 350.000 kroner fra Datatilsynet.

Bakgrunnen for varselet er urettmessig utlevering av data fra et forskningsprosjekt som hadde konsesjon fra Datatilsynet. Universitetet i Bergen er databehandlingsansvarlig for prosjektet. Det ble inngått avtaler og utlevert data til forskere ved Universitetet i Oslo, Høyskolen i Oslo og Akershus og Folkehelseinstituttet, uten at det var rettslig grunnlag for det.

Avviket ble avdekket i forbindelse med at Personvernombudet for forskning (NSD) skulle bistå det aktuelle forskningsprosjektet med søknad om forlengelse av konsesjon. Universitetet i Bergen meldte fra om avviket til Datatilsynet.

Datatilsynet har varslet om at de vil fatte følgende pålegg:

1. Universitetet i Bergen pålegges i medhold av personopplysningsloven § 46 første ledd å betale overtredelsesgebyr stort kroner 350.000 –femhundretusen-¹ for overtredelse av helseregisterloven §§ 6, 7, 17 og 22 og personopplysningsloven §§ 9, 11 og 33 ved urettmessig utlevering av helseopplysninger og mangelfull oppfyllelse av krav om internkontroll.
2. Universitetet i Bergen pålegges med hjemmel i helseforskningsloven § 52 å utarbeide dokumentasjon på internkontroll for forskning i tråd med helseforskningsloven § 6 annet ledd og forskrift om organisering av medisinsk og helsefaglig forskning § 4.
3. Universitetet i Bergen pålegges å informere allmennheten om avviket i tråd med helseregisterloven § 24.

Datatilsynet har i korte trekk funnet at UiB er ansvarlig for utlevering av helseopplysninger uten rettslig grunnlag, mangelfull implementering av internkontroll og mangelfull opplæring av prosjektledere og andre i den forskningsansvarliges virksomhet, samt utlevering av helseopplysninger i strid med pålagt taushetsplikt.

¹ Ved en inkurie er det ikke samsvar mellom beløpet skrevet med tall og bokstaver. Datatilsynet har bekreftet at 350.000 kroner er riktig beløp.

Datatilsynet presiserer at UiB har utvist åpenhet i saken, meldt avvik i tråd med regelverket, uoppfordret gitt utfyllende opplysninger og gjort det de kan for å begrense skade etter at de ble oppmerksom på avviket.

Ved fastsettelsen av gebyrets størrelse har Datatilsynet blant annet vektlagt at UiB i 2012 ble ilagt et overtredelsesgebyr på 250.000,- for behandling av sensitive personopplysninger uten rettslig grunnlag og manglende internkontroll.

Datatilsynet har gitt frist til 1. september 2015 for å kommentere varselet og komme med tilbakemelding på en hensiktsmessig frist for gjennomføring av varselet pålegg 2.

Universitetsdirektøren sine kommentarer

Universitetsstyret vedtok i sak 53/12 «Mål og strategidokument for helsefaglig forskning og for behandling av personopplysninger i forskning». Nytt internkontrollsystem trådte i kraft 1. februar 2013. Det er sterkt beklagelig at dette avviket har skjedd og det viser at internkontrollsystemet ikke har fungert godt nok.

Avviket skjedde ved at det ble inngått avtaler og utlevert data til delprosjekter ved andre institusjoner, uten at det ble fanget opp at nødvendige tillatelser manglet. Vi ser at det er behov for mer informasjon og bedre opplæring om hva som gir lovlig grunnlag for utlevering av data, både til forskere og til forskningsadministrasjonen. Vi ser også at rutinen for utlevering av forskningsdata må tydeliggjøres og forbedres.

UiB vil gå gjennom internkontrollsystemet og implementeringen av dette, for å identifisere og utbedre manglene. Vi må sikre at rutinene er gode nok og konkrete nok til å forhindre at slike avvik skjer igjen. Det er også nødvendig å sikre at alle som arbeider med helseopplysninger, andre typer registerdata og sensitive data, har tilstrekkelig kompetanse på regelverket og at forskerne får den administrative støtten de har behov for i arbeidet.

UiB vil ikke bestride gebyret Datatilsynet har varslet. Allmennheten er informert om avviket ved informasjon på UiB sine nettsider.

Med disse kommentarer fremmes følgende forslag til

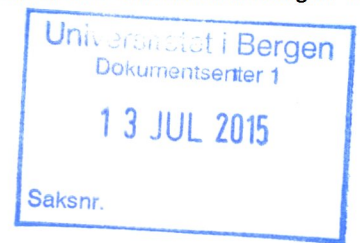
vedtak:

Universitetsstyret tar saken til etterretning

Kjell Bernstrøm
universitetsdirektør

18.08.2015/Silje Christine Nerheim

Vedlegg:
Varsel om vedtak og varsel om overtredelsesgebyr, datert 8.7.2015



Universitetet i Bergen
Herman Fossgate 6
5007 BERGEN

Deres referanse
2014/9326-SILNE

Vår referanse
14/01048-5/GRA

Dato
08.07.2015

Varsel om vedtak og varsel om overtredelsesgebyr – Uautorisert utlevering av forskningsdata

Datatilsynet viser til avviksmelding fra Universitetet i Bergen (UiB) datert 16. desember 2014, samt foreløpige meldinger datert 15. september 2014 og 17. september 2014

Datatilsynet beklager på det sterkeste at det har tatt lang tid å behandle saken.

Sakens bakgrunn

Saken gjelder en urettmessig utlevering av data fra prosjektet «*Innvandrerhelse fra begge sider: Pasienter og leger med innvandrerbakgrunn i primærhelsetjenesten*» som fikk konsesjon fra Datatilsynet 10. mai 2010 (Datatilsynets saksnummer 10/00069-6). Prosjektet er en registerstudie med hele befolkningen som utvalg.

Konsesjonen dekker kobling av data fra Reseptregisteret med opplysninger fra Fastlegedatabasen, Folkeregisteret, Helfo og Medisinsk fødselsregister. Konsesjonen ble gitt under forutsetning at Reseptregisterforskriftens krav til pseudonymitet ble ivaretatt.

Prosjektet ble utvidet i 2012 slik at konsesjonen også dekker underprosjektet «*Obsteriske problemstillinger blant kvinner med innvandrerbakgrunn*». Konsesjonen er forlenget i 2015 med endelig sluttdato 31. desember 2016.

Prosjektet har også forhåndsgodkjenning fra REK (2009/1747) med tilhørende utvidelser og forlengelse til 2016.

Databehandlingsansvarlig for prosjektet er Universitetet i Bergen.

Avviket som er meldt til Datatilsynet består i at det er inngått tre avtaler med eksterne forskere om utlevering av data fra forskningsfilen tilhørende ovennevnte prosjekt. Avviket ble avdekket i forbindelse med at Personvernombudet for forskning (NSD) skulle bistå prosjektet med søknad om forlengelse av konsesjon. I dialog mellom NSD og prosjektleder ble det klart at det var utlevert data fra prosjektet uten at det forelå rettslig grunnlag for slik utlevering. Virksomhetene som hadde mottatt data var Universitetet i Oslo (UiO), Høgskolen i Oslo og Akershus (HiOA) og Folkehelseinstituttet (FHI). Prosjektleder varslet sin leder som igjen varslet ledelsen ved UiB om avviket.

Da avviket ble gjort kjent for ledelsen ved UiB ble det sendt ut varsel til mottakerne om at datasettene måtte slettes. UiB har mottatt bekreftelse på at alle virksomhetene har slettet sine datasett.

Basert på sakens dokumenter og undersøkelser av egne arkiver, samt søk i REKs prosjektdatabaser kan vi ikke se at det finnes verken konsesjoner eller REK godkjenninger for de prosjekter det er utlevert data til. Dette betyr at avviket ikke bare gjelder UiB, men at det også innebærer avvik hos de instanser som har mottatt data. Datatilsynet har ikke mottatt avviksmeldinger fra disse virksomhetene.

Avviket er derfor todelt.

Den første delen av avviket er den urettmessige utleveringen som ble gjort i regi UiB. UiB hadde behandlingsgrunnlag som dekket behandling av dataene i et konkret forskningsprosjekt. UiB har ikke behandlingsgrunnlag som dekker utlevering av data fra dette prosjektet til eksterne prosjekter. Behandlingsgrunnlaget omfatter heller ikke eksterne forskerne, da det i forbindelse med søknad om konsesjon og REK-godkjenning ikke er opplyst at prosjektet er et samarbeidsprosjekt eller en multisenterstudie.

Utlevering av sensitive personopplysninger i strid med eksisterende behandlingsgrunnlag anses som brudd på grunnleggende bestemmelser om taushetsplikt og den behandlingsansvarliges plikt til å sørge for at personopplysninger ikke kommer på avveie eller utleveres til noen som ikke har nødvendig behandlingsgrunnlag. UiB plikter å sikre at slike avvik ikke skjer ved å sørge implementering av internkontroll for forskning. Avviket skyldes mangelfull oppfyllelse av denne plikten.

Den andre delen av avviket består i at henholdsvis UiO, HiOA og FHI tilsynelatende har behandlet helseopplysninger uten nødvendig behandlingsgrunnlag. Dette avviket indikerer også overtredelse av helseregisterloven § 7 og personopplysningsloven § 33, samt helseforskningsloven § 33. Datatilsynet vil behandle disse avvikene separat.

UiB's håndtering av avviket

Datatilsynet ønsker å presisere at UiB har utvist åpenhet i saken, meldt avvik i tråd med regelverket og uoppfordret gitt utfyllende opplysninger om avviket så snart ledelsen ved UiB ble gjort kjent med avviket. UiB har også gjort det de kan for å begrense skaden etter at de ble oppmerksomme på avviket.

Når det gjelder tiltak iverksatt for å minimere konsekvensene av avviket fremgår det av korrespondanse i saken at UiB har mottatt bekreftelse om at forskningsfilene er slettet fra alle de tre mottakerinstitusjonene.

UiB har beholdt kopier av de spesialtilpassede filene slik at de kan levres ut på nytt dersom nødvendige godkjenninger kommer i orden.

UiB innrømmer i sin avviksmelding at det er behov for mer informasjon og bedre opplæring om hva som gir lovlig grunnlag for utlevering av data, både til forskere og til forskningsadministrasjon. De ser også etter gjennomgang av internkontrollsystemet at rutiner for utlevering av forskningsdata kan tydeliggjøres og forbedres. De vil også vurdere om enkelte andre rutiner for kontroll med forskningsprosjekter bør oppdateres. Universitetsstyret har vedtatt at det i løpet av våren 2015 skal gjennomføres et prosjekt med fokus på å kartlegge og vurdere om det er etablert tilstrekkelige rutiner for behandling og oppbevaring av personopplysninger i forskning og helseforskning. Internrevisjonen vil også teste etterlevelse.

Det er videre opplyst om at det medisinske odontologiske fakultet arbeider med å forbedre rutineene for informasjonsflyt mellom forskere, institutt og fakultet for prosjekter som behandler sensitive personopplysninger.

Videre opplyser instituttet at de holder på å bygge opp en kjernefasilitet for biostatistikk og dataanalyse som skal gi tjenester til lokale forskere. Kjernefasiliteten har ansatt en person som skal ha kompetanse på forvaltning av forskningsdata og som skal kunne gi råd til universitetets registerforskere.

For å øke datasikkerheten arbeider universitetet med en sikker serverløsning som skal gi forskere tilgang til data uten at forskerne har dem på egne datamaskiner. Systemet kalles LPS. Systemet opplyses å være i en pilotfase, men er brukt i en rekke prosjekter. I fremtiden er planen at forskere gis kontrollert tilgang til forskningsdata i stedet for at data leveres ut til forsker.

UiB har vurdert det slik at det ikke er nødvendig å varsle allmennheten om avviket.

Datatilsynets tilsynskompetanse

Datatilsynet skal behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette jf. personopplysningsloven §§ 42 og 46.

Datatilsynets tilsynskompetanse gjelder for behandling av helseopplysninger etter helseregisterloven § 26 og helseforskningsloven jf § 47. Datatilsynets kompetanse etter helseforskningsloven er å føre tilsyn med bruken av helseopplysninger etter loven. Krav om forsvarlig organisering av forskning og forskningsansvarliges plikt til å ha internkontroll er viktige forutsetninger for at forskning på helseopplysninger kan tillates. Datatilsynet legger derfor til grunn at tilsynskompetansen etter helseforskningsloven også gjelder for bestemmelser som har betydning for forsvarlig behandling av helseopplysninger.

Datatilsynets vurdering av avviket ved UiB

Den 1. januar 2015 trådte ny helseregisterlov i kraft og helseregisterloven av 2001 ble opphevet. Avviket er vurdert etter tidligere helseregisterlov. Datatilsynets vedtak vil imidlertid vurderes etter ny helseregisterlov. I vår vurdering viser vi til det regelverket som er gjeldende på vedtakstidspunktet, men med henvisning til det regelverket som gjaldt da avviket fant sted i parentes. Vi vurderer at lovendringene ikke har betydning for det materielle innholdet i vår vurdering eller vedtak som fattes i saken.

Behandlingsgrunnlag

Behandling av helseopplysninger krever behandlingsgrunnlag. Det kan være konsesjon iht. personopplysningsloven § 33 og helseregisterloven § 7 (§ 5). Når formålet med behandlingen er medisinsk- og helsefaglig forskning kreves behandlingsgrunnlag i form av forhåndsgodkjenning fra REK, jf. helseforskningsloven § 33. Avviket i denne saken består i at det er utlevert sensitive opplysninger som bare kan behandles dersom det foreligger konsesjon fra Datatilsynet og forhåndsgodkjenning fra REK. Konsesjonsplikten følger av reseptregisterforskriften § 5-3 annet ledd.

Utlevering av helseopplysninger er å anse som en behandling av helseopplysninger jf. helseregisterloven § 2c). Hvorvidt det er tillatt å utlevere opplysninger avhenger av den databehandlingsansvarliges behandlingsgrunnlag. En utlevering av helseopplysninger krever også at mottaker av opplysningene har tillatelse til å behandle dem.

Det vises til helseregisterloven § 6 og helseforskningsloven § 34. Helseopplysninger kan bare behandles, sammenstilles og utleveres i tråd med forskningsprosjektets formål, eventuelle samtykker, behandlingsgrunnlaget etter helseforskningsloven § 33 og i samsvar med forskningsprotokollen jf. helseforskningsloven § 34 første ledd.

Sammenstilling og utlevering av helseopplysninger kan skje til databehandlingsansvarlige eller forskningsansvarlige som har særskilt behandlingsgrunnlag for å motta og behandle opplysningene. Slikt behandlingsgrunnlag kan være konsesjon eller hjemmel i lov eller forskrift, jf. helseforskningsloven § 34 tredje ledd.

Utleveringen innebærer dermed overtredelse av helseregisterloven §§ 6 og 7 og personopplysningsloven § 33, samt helseforskningsloven § 34, jf. § 33.

Internkontroll

Helseregisterloven § 22 (§ 17) omhandler den behandlingsansvarliges plikt til å etablere og holde ved like planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av loven. Utfyllende krav til innholdet i internkontrollen fremgår av personopplysningsforskriften kapittel 3.

I helseforskningsloven § 6 annet ledd stilles det også krav om at det skal føres internkontroll tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

I forskrift om organisering av medisinsk og helsefaglig forskning § 4 er kravene til internkontroll nærmere presisert. Det følger av bestemmelsen at den forskningsansvarlige skal sørge for

- at virksomhetens mål for forskningen, samt ansvars – og myndighetsforhold og hvordan forskningsvirksomheten strukturelt er tilrettelagt og organisert, er beskrevet
- at det føres løpende oversikt over alle medisinsk og helsefaglige forskningsprosjekter som involverer (...) helseopplysninger innen eget ansvarsområde,
- å ha oversikt over de krav i og i medhold av helseforskningsloven og annet regelverk, som gjelder for forskningen,
- at det utarbeides og dokumenteres rutiner som setter prosjektleder og medarbeidere i virksomheten i stand til å overholde kravene som nevnt (i punktet over)

- at prosjektleder, medarbeidere og annet personell som er involvert i forskningsprosjektet har nødvendig kompetanse
- at det utarbeides og dokumenteres rutiner for å motta meldinger om avvik og sikre at avvik rettes,
- at det foretas systematisk overvåkning og gjennomgang av internkontroll, for å sikre at den fungerer som forutsatt og bidrar til kontinuerlig forbedring i virksomheten.

Den forskningsansvarlige kan delegere oppgaver til andre, men ikke ansvar.

I avviksmeldingen er det forklart at prosjektleder hadde misforstått regelverket og at hun var i god tro da det ble inngått avtaler om utlevering av data. Misforståelsen i seg selv vitner om mangelfull kjennskap til regelverket og mangelfull forståelse av rekkevidden til et behandlingsgrunnlag, som konsesjon og forhåndsgodkjenning fra REK. Misforståelsen i seg selv vitner om at UiB ikke har oppfylt sin plikt til å sørge for at det finnes dokumenterte rutiner som setter prosjektleder i stand til å ha nødvendig oversikt over de lovkrav som gjelder for behandling av helseopplysninger i forbindelse med forskning. Dersom slike rutiner finnes, er det ikke gjort nok for å sikre at de ansatte kjenner til dem.

I tillegg fremgår det av sakens opplysninger at det er inngått tre separate avtaler om utlevering av forskningsdata tilhørende virksomhetens prosjekter, uten at noen har vurdert om utleveringen er tillatt, eller om mottaker har nødvendig behandlingsgrunnlag. Alle avtalene er signert av forskjellige ansatte ved UiB med fullmakt til å inngå avtaler med eksterne virksomheter.

Datatilsynets vurdering er at UiB ikke har oppfylt sine plikter når det gjelder å sørge for at prosjektleder og andre ansatte som er involvert i behandling av helseopplysninger har nødvendig kompetanse om gjeldende regelverk.

Mangelfull implementering av internkontroll innebærer overtredelse av helseregisterloven § 22 (17), helseforskningsloven § 6 annet ledd og forskrift om organisering av medisinsk og helsefaglig forskning § 4.

Organisering av forskning

Helseforskningsloven § 6 og forskrift om organisering av medisinsk og helsefaglig forskning §§ 3 og 5 inneholder bestemmelser om hvilke plikter den forskningsansvarlige og prosjektleder har etter loven.

I forskriftens § 6 er det fastsatt krav til forskningssamarbeid, eller såkalte multisenterstudier.

Multisenterstudier er definert som forskningsprosjekter som finner sted ved flere virksomheter samtidig og etter samme protokoll.

I annet ledd presiseres at en multisenterstudie skal ha én prosjektleder. Prosjektleder skal koordinere aktivitetene og sørge for å innhente forhåndsgodkjenning fra REK, og sikre at den forskningsansvarlige ved de øvrige deltakende virksomheter er informert om forskningsprosjektet før prosjektet startes. Forskriftens § 5 om prosjektleders plikter gjelder så langt den passer for prosjektleder i en multisenterstudie jf. tredje ledd.

Datatilsynet legger til grunn at avtaleformen som UiB har benyttet som grunnlag for utlevering av forskningsdata ikke oppfyller helseforskningslovens krav til et forskningssamarbeid og at avtalene ikke innebærer at mottaker av data omfattes av UiB's behandlingsgrunnlag.

Datatilsynets vurdering er derfor at utleveringene som fant sted ikke skjedde som en del av et forskningssamarbeid, og at avviket også er i strid med helseforskningslovens krav til organisering av forskning, fj. Helseforskningsloven §§ 3-6.

Taushetsplikt

Helseforskningsloven § 7: Enhver som får tilgang til helseopplysninger og andre personopplysninger som blir behandlet i et forskningsprosjekt skal hindre at andre får adgang eller kjennskap til opplysningene.

Helseregisterloven § 17 (15) jf. reseptregisterforskriften § 4-4: Enhver som behandler helseopplysninger etter denne loven har taushetsplikt etter helsepersonelloven §§ 21 flg. (forvaltningsloven §§ 13 til 13 e og helsepersonelloven).

Datatilsynet legger til grunn at avviket også er i strid med taushetspliktbestemmelsene i helseregisterloven § 17 (15) og helseforskningsloven § 7.

Håndtering av avvik

Avviket ble ikke fanget opp som følge virksomhetens internkontroll, men ble oppdaget av NSD i forbindelse med deres bistand ved søknad om forlengelse av konsesjon. På dette tidspunktet var avtalene inngått og data utlevert uten at avviket ble fanget opp ved UiB. Dette er en indikasjon på at virksomhetens system for å avdekke avvik ved behandling av personopplysninger fortsatt ikke fungerer godt nok.

Konklusjon

Datatilsynets vurdering av avviket er at UiB er ansvarlig for følgende overtredelser:

- Utlevering av helseopplysninger uten rettslig grunnlag anses som brudd på helseregisterloven §§ 6 og 7 (5) og personopplysningsloven §§ 9, 11 og 33. Utleveringen er også i strid med helseforskningsloven §§ 33 og 34.
- Mangelfull implementering av internkontroll og mangelfull opplæring av prosjektledere og andre i den forskningsansvarliges virksomhet anses som brudd på helseforskningsloven § 6 og forskrift om organisering av medisinsk og helsefaglig forskning §§ 3-5 og helseregisterloven § 22 (§ 17), personopplysningsloven § 33 og personopplysningsforskriften § 3-1.
- Utlevering av helseopplysninger i strid med pålagt taushetsplikt anses som brudd på helseforskningsloven § 7 og helseregisterloven § 17 og reseptregisterforskriften § 4-4.

Overtredelsesgebyr

I tråd med personopplysningsloven § 46 har Datatilsynet vurdert hvorvidt overtredelse av helseregisterloven §§ 6, 7, 17 og 22, personopplysningsloven §§ 9, 11 og 33 bør medføre et overtredelsesgebyr.

Adgangen til å ilegge overtredelsesgebyr er gitt som virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven og helseregisterloven. Internrettslig er overtredelsesgebyr ikke å anse som straff, men en administrativ sanksjon. Det må imidlertid antas at overtredelsesgebyr er å anse som straff etter EMK artikkel 6. I samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556 med videre henvisninger, legger derfor Datatilsynet til grunn at det kreves klar sannsynlighetsovervekt for lovovertrødelse for å kunne ilegge gebyr. Saksforholdet og spørsmålet om å ilegge overtredelsesgebyr er vurdert med utgangspunkt i dette beviskravet.

I vurderingen av om overtredelsesgebyr skal ilegges skal det særlig legges vekt på momentene som er listet opp i personopplysningsloven § 46 annet ledd bokstav a-h.

a) Hvor alvorlig overtredelsen har krenket de interesser loven verner

Datatilsynet anser det som svært alvorlig at UiB som er en profesjonell forskningsinstitusjon og forvalter store mengder forskningsdata ikke har sørget for tilstrekkelig implementering av et tilfredsstillende system for internkontroll. Tilsynet anser det også som svært alvorlig at prosjektledere og andre ansatte med fullmakt til å inngå avtaler om utlevering av data ikke har nødvendig kompetanse om regelverket som gjelder for behandling av forskningsdata.

At avviket skjedde har ikke hatt direkte konsekvenser for de registrertes personvern. Det samme datamaterialet kunne vært utlevert til flere virksomheter, enten ved at de hadde bedt om en ny forskningsfil, eller om de hadde fått tillatelse til å bruke den eksisterende filen. Dersom avviket ikke hadde blitt oppdaget, kunne det fått konsekvenser i forhold til de registrertes rettigheter. Det er uklart om UiB ville hatt oversikt over utleveringen og om de kunne ha oppfylt informasjonsplikten overfor de registrerte ved en eventuell henvendelse. Dette er i så fall også en konsekvens av manglende internkontroll og ville vært en følgefeil av den urettmessige utleveringen.

Datatilsynet legger allikevel til grunn at all behandling av sensitive personopplysninger uten rettslig grunnlag innebærer en krenkelse av personvernet til de registrerte. Når det gis tillatelse til å benytte slike opplysninger til konkrete formål er det basert på en avveining der samfunnsnyten ved at behandling tillates vurderes som mer tungtveiende enn hensynet til den enkeltes personvern. I en slik avveining er tillagt stor vekt at den behandlingsansvarlige blant annet begrenser tilgangen til opplysningene og at i tråd med gjeldende tillatelser og overordnet regelverk. Når virksomheten er en profesjonell forskningsinstitusjon har godkjenningmyndighetene og samfunnet for øvrig tillit til at integriteten til de registrerte ivaretas på en tilfredsstillende måte.

b) Graden av skyld

Det fremkommer av forarbeidene til bestemmelsen (Ot.prp. nr. 72 (2007-2008) Om lov om endring i personopplysningsloven mv.) at det med graden av skyld siktes til hvor

klandreverdigg handlingen er, for eksempel om den bærer preg av uhell eller om den har et mer systematisk eller planmessig preg.

I denne saken er det uomtvistelig at UiB både som databehandlingsansvarlig og som forskningsansvarlig har plikt til å sørge for at forskningsdata behandles i tråd med gjeldende regelverk. Oppgaver kan delegeres, men ikke ansvar.

Datatilsynet finner det klart at UiB er ansvarlig for avviket og at avviket ikke skyldes forhold utenfor virksomhetens kontroll.

c) Om overtrederen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen

UiB har beskrevet en rekke tiltak for å forbedre rutiner og internkontroll for forskning. Tilsynet har forståelse for at det kan ta tid å etablere nye systemer, men kravene om interkontroll for forskning etter helseforskningsloven har vært gjeldende fra 2009 og kravene om internkontroll etter personopplysningsloven har vært gjeldende siden 2001. Datatilsynets vurdering er at disse rutinene burde vært implementert i virksomheten for lenge siden.

Datatilsynet legger til grunn at avviket kunne vært unngått dersom virksomheten hadde hatt et tilfredsstillende system for opplæring av prosjektledere og andre ansatte som handler på vegne av den databehandlingsansvarlige/forskningsansvarlige.

f) Om det foreligger gjentakelse

Datatilsynet finner det spesielt bekymringsverdig at tilsynet i 2012 i sak 11/01072 ila UiB et overtredelsesgebyr på 250.000,- for behandling av sensitive personopplysninger uten rettslig grunnlag og manglende internkontroll. I UiB sitt brev til Datatilsynet (11/01072-9) uttalte UiB den gang følgende:

«I lys av denne saken vil vi gjennomgå alle sider ved vårt internkontrollsystem og vurdere om det er mulig å iverksette tiltak for ytterligere å forebygge brudd på regelverket. Det kan være aktuelt å innføre faste rutiner for å gjennomføre ytterligere kontroll etter gitte kriterier for å avklare om det er samsvar mellom godkjenninger og de dataene forsker faktisk behandler. Det er også viktig å vurdere samhandlingen mellom nivåene i organisasjonen i slike saker. UiB vil samarbeide med personvernombudet om dette.»

h) Overtrederens økonomisk evne

Datatilsynet legger til grunn at Universitetet i Bergen har solid økonomisk bæreevne.

Oppsummering

Etter en helhetlig vurdering er Datatilsynet kommet frem til at overtredelsesgebyr skal ilegges. I vurderingen er det lagt stor vekt på alvorlighetsgraden i at universitetet ikke har sørget for tilstrekkelig internkontroll og at manglende kontroll har ført til alvorlige brudd på grunnleggende krav i regelverket. Det er svært positivt at universitetet har varslet om avviket og bidratt til å klargjøre sakens faktum. Det er allikevel slik at avviket representerer overtredelse av helt grunnleggende bestemmelser om behandling av helseopplysninger og

faktum i saken viser at avviket ikke fanges opp gjennom internkontrollen til tross for at flere personer på ulike nivåer i organisasjonen har vært involvert.

Det er også tillagt vekt at avviket kunne vært unngått dersom UiB hadde sørget for tilstrekkelig implementering av internkontroll.

Ved fastsettelsen av gebyrets størrelse er det tillagt stor vekt at det foreligger gjentakelse.

I henhold til ovennevnte og i samsvar med Datatilsynets praksis, settes overtredelsesgebyret til NOK 350.000,-

Pålegg om dokumentasjonsplikt

Med hjemmel i helseforskningsloven § 52 og personopplysningsloven § 46 fjerde ledd har Datatilsynet vurdert om det skal gis pålegg om at behandling av helseopplysninger i strid med bestemmelsene i helseforskningsloven skal opphøre.

Datatilsynets vurdering er at den urettmessige behandlingen som skjedde i forbindelse med avviket er avsluttet. Vi finner allikevel at UiB ikke oppfyller sin plikt som forskningsansvarlig virksomhet når det ikke foreligger tilfredsstillende internkontroll for den behandlingen av helseopplysninger som skjer med hjemmel i helseforskningsloven og helseregisterloven.

Vi ser det som uforholdsmessig tyngende å pålegge UiB å stanse behandling av helseopplysninger i forskningsprosjekter inntil et tilfredsstillende system er implementert. Vi vurderer det derimot som nødvendig å pålegge UiB å dokumentere at de oppfyller helseforskningslovens krav til organisering av forskning og internkontroll, både når det gjelder å ha et dokumenterbart system og når det gjelder implementering i virksomheten. I dette ligger at det må fremlegges dokumentasjon på at det er etablert rutiner for opplæring av prosjektledere og andre som har arbeidsoppgaver relatert til behandling av helseopplysninger i forbindelse med forskning.

Informasjon til allmennheten

Retten til informasjon om behandling av helse- og personopplysninger er en grunnleggende rettighet etter helseregisterloven §§ 20-24 og personopplysningsloven §§ 18-22. Unntak fra retten til informasjon etter helseregisterloven er regulert i § 24, 2. ledd.

Ordlyden legger opp til en forholdsmessighetsvurdering der de registrertes nytte av å få kunnskap om behandlingen må avveies mot hvor byrdefull informasjonsplikten må sies å være for virksomheten. Også forarbeidene til helseregisterloven støtter opp om at det er en konkret vurdering av disse to hensyn som skal foretas.

UiB har gjort en vurdering av plikten til å informere de registrerte om den urettmessige utleveringen som er foretatt. Etter UiBs vurdering anses det ikke for hensiktsmessig å gi slik informasjon. UiB begrunner dette med at forskningsfilen i denne saken er pseudonym. Det betyr at universitetet ikke har tilgang til forskningsdeltakernes identitet. Individuell informasjon er derfor ikke mulig å gi.

Når det gjelder informasjon til allmennheten vurderer UiB slik informasjon som uhensiktsmessig fordi risikoen for identifikasjon av enkeltindivider har vært liten og at utleveringen har vært avtaleregulert. Mottakerne har blitt bedt om å slette dataene og det arbeides tiltak som skal forhindre liknende avvik i fremtiden.

Datatilsynet er ikke enig i at det er uhensiktsmessig å informere allmennheten om avviket. Avidentifisering og pseudonymisering av helseopplysninger er et av flere virkemidler som benyttes nettopp for å minimere risikoen for store personvernkonsekvenser dersom forskningsdata kommer på avveie. Selv om datasett er avidentifisert fritar ikke dette den databehandlingsansvarliges fra plikten til å sørge for at data ikke kommer på avveie i første omgang. Sikker lagring og begrenset tilgangskontroll skal sikre at dataene kun er tilgjengelige for de som trenger det, til konkrete formål. I denne saken har avidentifisering fungert etter formålet nettopp ved at konsekvensen av avviket ble begrenset. Vi mener allikevel at avviket avdekker en uakseptabel svikt i universitetets internkontroll.

Når svikt i interne rutiner fører til at forskningsdata kommer på avveie, betyr det at den tilliten samfunnet har til at forskningsdata behandles innenfor kontrollerte og sikre rammer ikke er berettiget. Det samme gjelder for den tilliten Datatilsynet og REK baserer sine avgjørelser på når det gis tillatelser til behandling av personopplysninger til forskning. I disse avgjørelsene tillegges det stor vekt at den forskningsansvarlige er en virksomhet som representerer et kompetent forskningsmiljø som kan forvalte sine tillatelser på en tilfredsstillende måte.

På samme måte som Datatilsynet pålegger forskningsinstitusjoner å informere om forskningsprosjekter blant annet via nettsider, mener vi at virksomheten skal informere om avvik som er av betydning for de registrerte. Informasjonen når ikke nødvendigvis ut til alle registrerte, men den tilgjengelig gjøres for de som er interessert.

Vi mener at informasjon til allmennheten er nødvendig for å opplyse de registrerte, som dette tilfellet er hele befolkningen, om hvordan opplysninger fra sentrale registre og andre offentlige kilder behandles. Økt kunnskap i befolkningen om bruk av personopplysninger vil kunne bidra til større grad av interesse for hvilke data som brukes, hvordan de brukes og risiko ved bruk. Informasjon vil også bidra til at de som er interessert i mer informasjon blir satt i stand til å benytte seg av sine rettigheter som bl.a innsyn, retting, sletting og eventuell reservasjon. Informasjon vil på denne måten gi bedre personvern for den enkelte.

Dersom forskningsinstitusjoner ikke pålegges å informere om at avvik skjer, vil den tilliten fra befolkningen som forskning ofte avhenger av, være basert på manglende kunnskap og uvitenhet om faktisk bruk av personopplysninger. Sett fra et personvernperspektiv er slik uvitenhet ikke i samsvar med samfunnets ønske om økt medvirkning fra den registrertes side, enten det dreier seg om bruk av helseopplysninger eller andre forskningsdata. Uvitenhet samsvarer heller ikke med utviklingen mot økt bruk av reservasjonsrett.

Offentliggjøring av avvik er ikke ressurskrevende for virksomheten. Nyten for allmennheten er stor i og med at informasjon bidrar til å øke befolkningens bevissthet samtidig som deres grunnleggende rett til å bli informert oppfylles så langt det er mulig. Retten til informasjon er avgjørende for de registrertes mulighet til å ivareta andre grunnleggende personvernrelaterte rettigheter.

Etter en konkret vurdering er Datatilsynet kommet til at de registrertes rett til å bli informert om at avvik skjer, veier tyngre enn hensynet til hvor byrdefullt det må sies å være for UiB å informere om avviket.

Varsel om vedtak

Dette er et varsel om at Datatilsynet vil fatte følgende pålegg:

1. Universitetet i Bergen pålegges i medhold av personopplysningsloven § 46 første ledd å betale overtredelsesgebyr stort kroner 350.000 – femhundretusen – for overtredelse av helseregisterloven §§ 6, 7, 17 og 22 og personopplysningsloven §§ 9, 11 og 33 ved urettmessig utlevering av helseopplysninger og mangelfull oppfyllelse av krav om internkontroll.
2. Universitetet i Bergen pålegges med hjemmel i helseforskningsloven § 52 å utarbeide dokumentasjon på internkontroll for forskning i tråd med helseforskningsloven § 6 annet ledd og forskrift om organisering av medisinsk og helsefaglig forskning § 4.
3. Universitetet i Bergen pålegges å informere allmennheten om avviket i tråd med helseregisterloven § 24.

Avsluttende merknader

Etter forvaltningslovens § 16 skal parten varsles og gis anledning til å uttale seg før endelig vedtak fattes. Dersom dere har kommentarer til dette varselet eller andre merknader i saken, ber vi om at dere sender dette til Datatilsynet senest **innen 1. september 2015** fra dags dato. Innen samme frist ber vi dere om å komme med en tilbakemelding på hensiktsmessig frist for gjennomføring av varselet pålegg 2.

Deres tilbakemelding vil være med på å danne grunnlag for et eventuelt endelig vedtak.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Grete Alhaug
seniorrådgiver

Kopi til: Statens Helsetilsyn. Postboks 8128 Dep. 0032 Oslo
Den nasjonale forskningsetiske komité for medisin og helsefag, Kongens
gate 14, 0153 Oslo
Folkehelseinstituttet - Personvernombudet, Postboks 4404 Nydalen, 0403
OSLO
Høgskolen i Oslo og Akershus, Postboks 4, 0130 OSLO
Universitetet i Oslo, Postboks 1072 Blindern, 0316 OSLO