Datatilsynet

Hordaland fylkeskommune
Postboks 7900
5020 BERGEN

Deres referanse	Vår referanse	Dato
2016/3926-11	16/00438-10/TJU	27.07.2016

Vedtak om pålegg og overtredelsesgebyr - Publisering av sensitive personopplysninger på Internett

1. Sakens bakgrunn

Saken gjelder publisering av sensitive personopplysninger på Internett. Et dokument fra klagebehandling i fylkeskommunen ble lagt ut i fulltekst på fylkeskommunens nettsider. Dokumentet inneholdt helseopplysninger om fem personer. Datatilsynet har varslet vedtak om pålegg og overtredelsesgebyr.

Avviket er nærmere beskrevet i punkt 3. Fylkeskommunen har kommet med tilsvar til vårt varsel, og vi vil derfor endre vedtaket noe. En forklaring til dette finnes i punkt 4. Begrunnelse for vedtaket følger i punkt 5. Informasjon om klageadgang finnes endelig i punkt 6.

2. Vedtak

Datatilsynet fatter med dette følgende vedtak om pålegg:

1. *Med hjemmel i personopplysningsloven § 46, jf. personopplysningsforskriften § 2-2, pålegges Hordaland fylkeskommune å iverksette tekniske sikkerhetstiltak for å begrense muligheten for at dokumenter unntatt offentlighet kan publiseres på Internett, jf. personopplysningsloven § 13, jf. personopplysningsforskriften § 2-14 første ledd.*

Datatilsynet fatter med dette følgende vedtak om overtredelsesgebyr:

2. *Med hjemmel i personopplysningsloven § 46 pålegges Hordaland fylkeskommune å betale et overtredelsesgebyr til statskassen stort kroner **150 000 – ett hundre og femti tusen** – for å ha behandlet personopplysninger uten behandlingsgrunnlag, jf. personopplysningsloven §§ 8 og 9, jf. 11 bokstav a, og for ikke å ha iverksatt tekniske sikkerhetstiltak for å begrense muligheten for at dokumenter unntatt offentlighet kan publiseres på Internett og etablert rutiner for å oppdage slik publisering, jf. personopplysningsloven § 13, jf. personopplysningsforskriften § 2-14 første ledd.*

Postadresse: Postboks 8177 Dep 0034 OSLO
Kontoradresse: Tollbugt 3
Telefon: 22 39 69 00
Telefaks: 22 42 23 50
Org.nr: 974 761 467
Hjemmeside: www.datatilsynet.no

3. Beskrivelse av avviket

Et dokument fra den fylkeskommunale klagenemd ble lagt ut i fulltekst på fylkeskommunens nettsider fra 26. mai 2015. Dokumentet inneholdt helseopplysninger om fem personer. Helseopplysningene var av en svært sensitiv art og inkluderte fysiske og psykiske diagnoser og personlige behov.

Publiseringen ble oppdaget ved at en av de berørte søkte på sitt eget navn på søkemotoren Google og derved fant dokumentene. Personen tok kontakt med fylkeskommunen, som fjernet dokumentene fra sine hjemmesider den 18. februar 2016. Datatilsynet ble først gjort oppmerksom på saken gjennom brev fra den berørte personen av 29. februar 2016.

Da Datatilsynet stadig ikke mottok avviksmelding etter personopplysningsforskriften § 2-6 tredje ledd, tok vi kontakt med fylkeskommunen ved personvernombudet den 14. mars 2016. Vi fikk opplyst at avviksmelding var under utarbeidelse. Den 22. mars 2016 hadde Datatilsynet fremdeles ikke mottatt avviksmelding og sendte fylkeskommunen krav om redegjørelse. Samme dag kontaktet vi personvernombudet for å påse at kravet ble fulgt opp. Kravet hadde frist 1. april 2016, men da redegjørelsen ble forsinket, kontaktet Datatilsynet fylkesrådmannen for å følge opp kravet 5. april 2016. Datatilsynet mottok redegjørelsen, som var datert 7. april 2016.

I redegjørelsen forklarer fylkeskommunen at publiseringen skyldtes at et saksdokument ikke ble korrekt avskjermet. Dokumentet var unntatt offentlighet i saksbehandlingssystemet Ephorte. Det ble deretter eksportert til et møteinnkallingsdokument. Når dette skjer, må imidlertid saksdokumentet avskjermes også i innkallingsdokumentet. Det er dette som ikke har skjedd.

Fylkeskommunen opplyser at søketreffet til dokumentet på Google ikke lenger er tilgjengelig. Vi forutsetter at dokumentet ikke er tilgjengelig gjennom andre søkemotorer.

Fylkeskommunen gjør videre rede for hvilke rutiner og risikovurderinger som ligger til grunn for behandling av denne typen personopplysninger og hvordan rutinene vil gjennomgås etter denne hendelsen. Fylkeskommunen skriver at en ekstra medarbeider være tilstede for å sjekke avskjerminger når man produserer møteinnkallinger der saker unntatt offentlighet inngår. Videre vil det i slike saker innføres manuell etterkontroll opp mot innsynsportalen for å påse at avskjermede dokumenter ikke har blitt publisert. Det vil bli innført tiltak for at møteinnkallinger og protokoller for møter i utvalg som behandler saker som inneholder personopplysninger, ikke publiseres. Møteinnkallinger og protokoller fra den fylkeskommunale klagenemd vil bli behandlet på annen måte enn for andre utvalg. Fylkeskommunen er i dialog med Ephorte for å finne tekniske sikkerhetstiltak.

Fylkeskommunen varslet de berørte en tid etter avviket ble oppdaget og tar selvkritikk for at varsling ikke fant sted tidligere.

4. Merknader til vedtaket

Fylkeskommunen har kommet med tilsvar til vårt varsel om vedtak.

For det første understreker fylkeskommunen at dokumenter i innsynsløsningen ikke er åpent tilgjengelige på Internett. De er derfor ikke er søkbare for søkemotorer. Av den grunn frafaller vi det varslede vedtaket om å pålegge fylkeskommunen å unngå at innsynsløsningen blir indeksert av søkemotorer (punkt 2 i varselet).

For det andre ber fylkeskommunen at dette også tas hensyn til i vurderingen av overtredelsesgebyrets størrelse. Overtredelsesgebyret bygger på at dokumentet ble publisert på Internett og at fylkeskommunen ikke hadde tilstrekkelige sikkerhetstiltak for å unngå og oppdage dette. At dokumenter generelt indekseres av søkemotorer har ikke vært et moment i vurderingen av om overtredelsesgebyr skal ilegges eller gebyrets størrelse. Vi nevner imidlertid at det aktuelle dokumentet faktisk ble indeksert av søkemotorer under vurderingen av om overtredelsesgebyr skal ilegges, under drøftelsen etter personopplysningsloven § 46 annet ledd bokstav a. Det er ikke omstridt at dette skjedde. Uansett har dette faktum lite å si for vurderingen av utmålingen. Det sentrale er at et dokument som ikke skulle publiseres, lå åpent på internett i ni måneder, og at dette skyldes manglende sikkerhetstiltak. Derfor vil det ikke påvirke gebyrets størrelse at det varslede pålegget om å unngå indeksering, frafalles.

For det tredje har fylkeskommunen gjort rede for hvilke sikkerhetstiltak man planlegger å iverksette for å unngå denne typen hendelser i fremtiden. Det er positivt at fylkeskommunen tar dette på alvor og finner gode løsninger. Vi kan imidlertid ikke se at arbeidet med å iverksette sikkerhetstiltak for å unngå at dokumenter unntatt offentlighet publiseres på Internett, er ferdigstilt. Derfor opprettholder vi det varslede vedtaket på dette punkt. Vi presiserer imidlertid begrunnelsen for vedtaket i tråd med informasjonen fra fylkeskommunen.

5. Begrunnelse for vedtaket

Behandlingsgrunnlag for publisering på nett
Offentlighetsloven § 10 tredje ledd og offentlighetsforskriften § 7 første ledd slår fast at virksomheter som er omfattet av loven kan publisere dokumenter for allmenheten på Internett. Det er opp til den enkelte virksomhet å bestemme om dette skal skje. Offentlighetsforskriften § 7 andre ledd regulerer hvilke personopplysninger som ikke kan publiseres på Internett. Blant annet vil dette gjelde opplysninger som er underlagt taushetsplikt og opplysninger som er sensitive etter personopplysningsloven § 2 nr. 8.

Personopplysningsloven § 6 første ledd sier at personopplysningsloven ikke begrenser innsynsrett etter offentlighetsloven. Det vil si at innsyn etter offentlighetsloven kan gis uten å vurdere om personopplysningslovens vilkår for behandling av personopplysninger er oppfylt. Spørsmålet er om dette stiller seg annerledes når dokumenter publiseres på Internett.

Justisdepartementets lovavdeling vurderte forholdet mellom personopplysningsloven og offentlighetsloven i sin uttalelse til Datatilsynet av 16. juli 2004. Uttalelsen knytter seg til offentlighetsloven av 1970, som siden har blitt erstattet av offentlighetsloven av 2006, men uttalelsen er fremdeles relevant. I punkt 4.3.2 uttaler man:

Det avgjørende i forhold til personopplysningsloven § 6 første ledd er imidlertid at offentlighetsloven ikke gir den enkelte noe krav på at innsyn i et dokument som er underlagt innsynsrett, skal gis ved å gjøre dokumentene tilgjengelig for enhver på internett (...) På denne bakgrunn antar Lovavdelingen at personopplysningsloven § 6 første ledd ikke gjelder når dokumenter som er underlagt innsynsrett legges ut på nettet.

Med andre ord vil personopplysningsloven gjelde i disse tilfellene, forutsatt at behandlingen faller innenfor personopplysningslovens virkeområde.

Denne saken handler om elektronisk behandling av dokumenter med taushetsbelagte opplysninger om helseforhold som kan knyttes til enkeltpersoner. Dette faller innenfor personopplysningslovens virkeområde, jf. § 3. Helseopplysninger er sensitive personopplysninger, jf. § 2 nr. 8.

For å publisere sensitive personopplysninger på Internett kreves et rettslig behandlingsgrunnlag etter personopplysningsloven §§ 8 og 9, jf. § 11 bokstav a. Offentlighetsloven § 10 og offentlighetsforskriften § 7 slår fast at taushetsbelagte opplysninger og sensitive personopplysninger ikke kan gjøres tilgjengelig på Internett. Etter Datatilsynets vurdering er dette et forbud mot publisering som diskvalifiserer behandlingsgrunnlagene etter § 8 bokstav a–f og § 9 bokstav c–h.

På denne bakgrunn finner Datatilsynet at Hordaland fylkeskommunes publisering av sensitive personopplysninger på Internett manglet behandlingsgrunnlag etter personopplysningsloven §§ 8 og 9, jf. § 11 bokstav a. Dette er et av grunnlagene for at fylkeskommunen ilegges overtredelsesgebyr.

Sikkerhetstiltak
Virksomheten har plikt til å iverksette planlagte og systematiske tiltak for å sørge for tilfredsstillende informasjonssikkerhet, jf. personopplysningsloven § 13. Personopplysningsforskriften § 2-14 første ledd tredje ledd pålegger virksomheten å iverksette sikkerhetstiltak for å hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Dette inkluderer tekniske tiltak for å unngå sikkerhetsbrudd og rutiner for å avdekke hendelser som kan forårsake sikkerhetsbrudd som to uavhengige tiltak.

Fylkeskommunen behandler en større mengde personopplysninger, og en del av personopplysningene som behandles er av sensitiv art. Konsekvensene av et avvik kan derfor være store. Dette stiller høyere krav til informasjonssikkerheten.

I fylkeskommunens saksbehandlingssystem måtte avskjerming av dokumenter til møteinnkallelser skje manuelt. Dokumenter som var avskjermet i saksdelen av saksbehandlingssystemet kunne uten videre publiseres. Fylkeskommunen hadde altså ikke tekniske tiltak for å unngå sikkerhetsbrudd. Videre fantes det ikke rutiner for å oppdage

sikkerhetsbrudd. Mangelen på slike sikkerhetstiltak på avvikstidspunktet er et av grunnlagene for at fylkeskommunen ilegges overtredelsesgebyr.

Fylkeskommunen iverksetter nå sikkerhetstiltak for å unngå og oppdage sikkerhetsbrudd. Når slike tiltak er iverksatt, vil kommunen følge personopplysningsforskriften § 2-14. Siden ikke alle tiltak ennå er iverksatt og dette kan ta noe tid, fatter vi vedtak om pålegg for å sikre at tiltakene iverksettes.

Generelt om internkontrollplikten
Et viktig formål bak personopplysningsloven er å ansvarliggjøre virksomheter for deres behandling av personopplysninger. Loven regulerer ikke bare *hvem* som er behandlingsansvarlig, men gir også nærmere pålegg om *hvordan* behandlingsansvaret skal ivaretas. Plikten til å etablere internkontroll er et slikt pålegg: Gjennom planlagte og systematiske tiltak skal den behandlingsansvarlige sette seg selv i stand til å sikre, kontrollere og dokumentere at virksomheten til enhver tid etterlever personopplysningslovens øvrige bestemmelser.

Et internkontrollsystem skal tilpasses den enkelte virksomhet ut fra type virksomhet, størrelse og behandlingen(e)s art og omfang, jf. personopplysningsforskriften § 3-1, jf. personopplysningsloven § 14. Internkontrollplikten innebærer at den behandlingsansvarlige *skal* ha kjennskap til gjeldende regler om behandling av personopplysninger og ha dokumenterte rutiner for oppfyllelse av plikter og rettigheter etter personopplysningsregelverket. Internkontrollplikten er først overholdt når rutinene er implementert, slik at de i praksis ligger til grunn for virksomhetens behandling av personopplysninger.

Datatilsynets vurdering av overtredelsesgebyr
Datatilsynet mener det er nødvendig å reagere på lovovertredelsene som er beskrevet over. I medhold av personopplysningsloven § 46 kan Datatilsynet ilegge overtredelsesgebyr. Vi siterer fra bestemmelsen:

> *Datatilsynet kan pålegge den som har overtrådt denne loven eller forskrifter i medhold av den, å betale et pengebeløp til statskassen (overtredelsesgebyr) på inntil 10 ganger grunnbeløpet i folketrygden. Fysiske personer kan bare ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser. Et foretak kan ikke ilegges overtredelsesgebyr dersom overtredelsen skyldes forhold utenfor foretakets kontroll.*
>
> *Ved vurderingen av om overtredelsesgebyr skal ilegges, og ved utmålingen, skal det særlig legges vekt på*
> - *a) hvor alvorlig overtredelsen har krenket de interesser loven verner,*
> - *b) graden av skyld,*
> - *c) om overtrederen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen,*
> - *d) om overtredelsen er begått for å fremme overtrederens interesser,*
> - *e) om overtrederen har hatt eller kunne ha oppnådd fordel ved overtredelsen,*

f) om det foreligger gjentakelse,
g) om andre reaksjoner som følge av overtredelsen blir ilagt overtrederen eller noen andre som har handlet på vegne av denne, blant annet om noen enkeltperson blir ilagt straff og
h) overtrederens økonomiske evne.

Bestemmelsen gir i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men annet ledd legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal ha særlig vekt.

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

Datatilsynet finner det klart at Hordaland fylkeskommune har behandlet personopplysninger uten behandlingsgrunnlag, jf. personopplysningsloven §§ 8 og 9, jf. 11 bokstav a, og at fylkeskommunen ikke hadde iverksatt tekniske sikkerhetstiltak for å begrense muligheten for at dokumenter unntatt offentlighet kan publiseres på Internett og etablert rutiner for å oppdage slik publisering, jf. personopplysningsloven § 13, jf. personopplysningsforskriften § 2-14 første ledd.

I vurderingen av om overtredelsesgebyr skal ilegges, legger Datatilsynet særlig vekt på at overtredelsene betydelig har krenket grunnleggende interesser som loven verner, jf. § 46 annet ledd bokstav a. Loven verner om grunnleggende personverninteresser som den personlige integritet og privatlivets fred, jf. lovens § 1.

Datatilsynet legger her særlig vekt på alvoret i at det ikke var adgang til å publisere sensitive personopplysninger etter personopplysningsloven § 11 bokstav a, jf. §§ 8 og 9. Brukerne av fylkeskommunens tjenester har en klar beskyttelsesverdig interesse mot publisering av konfidensielle opplysninger. Slik publisering kan få alvorlige konsekvenser for den enkelte både fordi omgivelsene får tilgang til informasjon som den registrerte ikke selv har valgt å gjøre kjent, men også fordi tilgjengeligheten på Internett gjør det uforutsigbart hvor mange som har skaffet seg informasjonen og om det er mulig å få slettet. Allmennpreventive grunner og hensynet til at reglene skal ha effekt og virke etter sin hensikt, taler da med styrke for at det reageres med et virkemiddel som overtredelsesgebyr.

Videre legger tilsynet stor vekt på alvoret i at personopplysningene var tilgjengelige i nesten ni måneder. Jo lenger personopplysningene ligger tilgjengelig på Internett, desto større er potensialet for uautorisert innsyn. Videre var personopplysningene tilgjengelige for søkemotorer, som førte til spredning.

Datatilsynet legger videre vekt på at det er noe å bebreide fylkeskommunen for det som har skjedd, jf. § 46 annet ledd bokstav b. For å opprettholde tillitsforholdet mellom forvaltning og borgere er forventningen at Hordaland fylkeskommune setter seg grundig inn i personopplysningsregelverket og etablerer gode rutiner for å sikre etterlevelsen av det. Det finnes dessuten mye veiledning utarbeidet for utøvelsen av offentlighet og meroffentlighet.

Datatilsynet legger også stor vekt på at avviket kunne ha forebygget overtredelsen ved tekniske tiltak og rutiner, jf. § 46 annet ledd bokstav c. Mangelen på tekniske tiltak resulterte i publiseringen av personopplysningene og utgjør i seg selv en overtredelse. Samtidig hadde ikke fylkeskommunen rutiner for å fange opp avvik – det var en av de berørte selv som oppdaget publiseringen. Det kan på denne bakgrunn heller ikke utelukkes at også andre avskjermede dokumenter ligger offentlig tilgjengelig.

Datatilsynet kjenner ikke til at det har blitt ilagt fylkeskommunen andre reaksjoner, jf. § 46 bokstav g.

Overtrederens økonomiske evne er det i liten grad lagt vekt på, jf. § 46, fjerde ledd bokstav h.

Datatilsynet kan ikke se at de øvrige momenter som loven fremhever gjør seg gjeldende i nevneverdig grad – verken i skjerpende eller formildende retning.

Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges.

Gebyrets størrelse
Når det gjelder gebyrets størrelse, skal de samme momentene som ved vurdering av om gebyr skal ilegges, tillegges særlig vekt. De forhold Datatilsynet har pekt på ovenfor taler for et gebyr av en viss størrelse. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken. Samtidig må gebyrets størrelse stå i et rimelig forhold til overtredelsen og virksomheten.

I motsetning til liknende saker, der offentlige organer har publisert én persons personopplysninger på Internett, har denne saken berørt fem personer. Videre har personopplysningene ligget tilgjengelig i nesten ni måneder. Denne saken er altså mer alvorlig, og dette taler for et noe høyere gebyr. Etter en totalvurdering av saken og graden av alvorlighet i overtredelsen, har vi kommet til at et overtredelsesgebyr på 150 000 kroner anses riktig.

6. Klageadgang

Dette er et enkeltvedtak som kan påklages etter forvaltningslovens regler, jf. forvaltningsloven § 28. Fristen for å klage er **tre uker** etter dette brevet er mottatt. En eventuell klage skal sendes til Datatilsynet. Personvernnemda er klageorgan.

Vennlig hilsen

Bjørn Erik Thon
direktør

Tobias Judin
rådgiver