Datatilsynet

Årdal kommune
Statsråd Evensensveg 4
6885 ÅRDALSTANGEN

Deres referanse	Vår referanse	Dato
16/189-23	16/00366-5/KBK	16.06.2016

Vedtak om pålegg og overtredelsesgebyr - Publisering av sensitive personopplysninger på offentlig postjournal - Årdal kommune

Det vises til varsel om vedtak og overtredelsesgebyr av 8. april 2016 og kommunens tilsvar av 25. april 2016.

Datatilsynet har vurdert tilsvaret fra kommunen, og er kommet til at overtredelsesgebyr fortsatt skal gis, men at beløpet justeres ned fra kr. 250.000 til kr. 150.000. Det vises til vår vurdering under kapittelet om gebyrets størrelse. Vedtaket om pålegg er også justert til både å omfatte organisatoriske og /eller tekniske sikkerhetstiltak, og ikke som varslet bare tekniske sikkerhetstiltak.

Sakens faktiske forhold
I forbindelse med et varslet tilsyn av Fylkesmannen i Hordaland innenfor området «spesialomsorg» ble det oversendt dokumentasjon på 15 brukere som mottar tjenester fra Årdal kommune. Spesialomsorg omfatter tjenester som psykiatri, psykisk helsetjeneste, botilbud for personer med psykisk utviklingshemming og barneboliger med heldøgnstilbud.

Dokumentasjonen ble sendt kryptert via meldingsutvekslingstjenesten «BEST» og inneholdt et generelt følgebrev og 2 vedlegg med underlagsdokumentasjon.

«BEST» er en løsning som baserer seg på sikker meldingsutveksling ved bruk av sertifikater mellom forskjellige NOARK-systemer. Det benyttes WebServicer for kommunikasjon internt innenfor egen organisasjon. Innholdet i e-posten krypteres før det blir sendt.

Hoveddokumentet var et generelt følgeskriv som ikke inneholdt taushetsbelagt informasjon. Begge vedleggene inneholdt imidlertid taushetsbelagte opplysninger og skulle vært unntatt offentlighet med hjemmel i offentleglova § 13. Vedlegg 1 ble unntatt offentlighet og kom ikke på postlista. Vedlegg 2 ble også besluttet unntatt offentlighet, men ble lagret på en måte som gjorde at dette ikke ble gjort gjeldende i publiseringsløsningen.

Konsekvensen av dette var at dokumentene som fremgikk av postlista var tilgjengelige i klartekst via en lenke, og sensitive personopplysninger om 15 brukere med nedsatt funksjonsevne lå tilgjengelig i ett døgn før det ble oppdaget. I dokumentet var det

opplysninger om fødselsnummer, kontonummer, diagnose, medisinbruk og personlige behov. Alle brukerne var over 18 år.

At dokumentene lå offentlig tilgjengelig ble oppdaget av en journalist i Sogn Avis, som kontaktet Fylkesmannen i Hordaland, som igjen tok kontakt med kommunen.

Årdal kommune har laget rutiner for kvalitetssikring av offentlig postliste på papir og på nett. Rutinene inneholder også krav om å kontrollere alle de aktive «linkene» i offentlig postliste på nettet, både hoveddokument og vedlegg.

I telefonsamtale mellom rådmann Olve Fossedal og Knut B. Kaspersen torsdag 10. mars 2016 ble det opplyst at kommunen tirsdag 8. mars 2016 hadde hatt et informasjonsmøte med alle vergene til de 15 psykisk utviklingshemmede. Kommunen har kommet til en minnelig ordning med de berørte, og disse har bekreftet at de anser seg ferdig med saken. I samtalen ba Datatilsynet også om å få tilgang til kommunens risikovurdering knyttet til publisering av postliste på nett. I brev av 15. mars 2016 ble kommunens rutiner og risikovurdering oversendt.

Vedtak om pålegg

1. Årdal kommune pålegges i medhold av § 46, fjerde ledd, å iverksette organisatoriske og/eller tekniske sikkerhetstiltak for å begrense muligheten for uautorisert publisering av dokumenter på Internett, i samsvar med personopplysningsloven § 13, jf. personopplysningsforskriften §§ 2-1, 2-2, 2-11 og 2-14.

Vedtak om overtredelsesgebyr

1. Årdal kommune pålegges i medhold av personopplysningslovens § 46, første ledd, jf. §§ 8, 9 13 og 14 å betale et overtredelsesgebyr til statskassen, stort kroner **150.000 – etthundreogfemtitusen**, for å ha behandlet personopplysninger uten behandlingsgrunnlag, jf. §§ 8 og 9, og uten å etablere tilfredsstillende tiltak for å hindre uautorisert tilgjengeliggjøring i personopplysninger hvor konfidensialitet er nødvendig, jf. forskriften § 2-11, og for ikke å ha gjennomført risikovurdering for å klarlegge sannsynligheten for, og konsekvenser av, sikkerhetsbrudd, jf. forskriften § 2-4 andre ledd.

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral, jf. § 47a.

Nærmere om internkontrollplikten - generelt

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. personopplysningsloven § 14, jf. personopplysningsforskriften § 3-1. 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.

Behandlingsgrunnlag for publisering på nett
Offentleglova § 10 tredje ledd og offentlegforskrifta § 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. Offentlegforskrifta § 7 andre ledd regulerer hvilke personopplysninger som ikke kan publiseres på Internett. Blant annet vil dette gjelde personopplysninger som er underlagt taushetsplikt, fødselsnummer og sensitive opplysninger som følger av personopplysningsloven § 2 nr. 8.

Når kommunen har bestemt at postjournal, med link til fulltekstdokumenter, skal publiseres på Internett, har den gjort et bevisst valg med hensyn til meroffentlighet. I en uttalelse til Dagens Næringsliv gir Justisdepartementets lovavdeling i brev av 16. august 2007 sin vurdering av forholdet mellom offentlighetsloven og personopplysningsloven:

> *«Personopplysningsloven kommer imidlertid til anvendelse når saksdokumentet ikke er underlagt innsynsrett, men hvor forvaltningen likevel har adgang til å gi innsyn ved å utøve meroffentlighet, jf. offentlighetsloven § 2 tredje ledd (nåværende § 11 vår anm.), forutsatt at man er innenfor personopplysningslovens anvendelsesområde for øvrig.»*

Dokumentet som ble lagt ut på Internett, var underlagt taushetsplikt fordi det inneholdt sensitive personopplysninger som diagnose, medisinbruk og informasjon om brukerens personlige behov. Fødselsnummeret til den enkelte bruker ble også publisert på Internett. Dette er innenfor personopplysningslovens anvendelsesområde, jf personopplysningslovens § 12.

Internkontrollen, som kommunen er pliktig til å etablere etter personopplysningsloven § 14, skal inneholde rutiner for «vurdering av formål med behandling av personopplysninger i samsvar med personopplysningsloven § 11 bokstav a» jf. personopplysningsforskriften § 3-1 tredje ledd bokstav b. Etter personopplysningsloven § 11 bokstav a kan det bare behandles personopplysninger når dette er tillatt etter § 8 og § 9. Dette innebærer at kommunen må ha behandlingsgrunnlag etter §§ 8 og 9 for å kunne publisere sensitive personopplysninger på Internett.

Offentleglova § 10 og offentlegsforskrifta § 7 fastslår at taushetsbelagte personopplysninger, sensitive personopplysninger og fødselsnummer ikke kan gjøres tilgjengelig på Internett. Etter Datatilsynets vurdering er dette et forbud mot publisering som diskvalifiserer de øvrige

behandlingsgrunnlagene som følger av personopplysningsloven (nødvendighetsvurderingene etter § 8 bokstav a-f og § 9 bokstav c-h).

Konklusjon:
Årdal kommunes publisering av sensitive personopplysninger på Internett mangler behandlingsgrunnlag etter personopplysningsloven § 11, jf §§ 8 og 9.

Rutinene for publisering av personopplysninger på nett
Årdal kommune har vedtak om å praktisere meroffentlighet (kommunestyrevedtak 057/10 Informasjonsreglementet), noe som betyr at kommunen i størst mulig grad skal legge til rette for offentlighet og innsyn i kommunen sine saksdokumenter. Datatilsynet mener at den utlevering av personopplysninger som har skjedd er et brudd på personopplysningsloven § 13, jf. personopplysningsforskriften § 2-11, som stiller krav til den behandlingsansvarlige om at det gjennomføres tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet. Årdal kommune har beskrevet at de har iverksatt organisatoriske tiltak, slik som gjennomgang av rutiner og opplæring, men det ser ikke ut til å være tilstrekkelig. Etter Datatilsynets vurdering er rutinene som er laget for å kvalitetssikre publisering av offentlig postliste på papir og nett for generelle. Slik rutinene er utformet vil de ikke i tilstrekkelig grad hindre tilgjengeliggjøring av dokumenter som ikke skal publiseres. Det er kontrollen av linker til fulltekstdokumentet som har sviktet. Denne kontrollen skjer manuelt og uten særskilt kvalitetssikring. Rutinene må synliggjøre de kritiske fasene ved publiseringen og hva medarbeiderne må være særskilt oppmerksomme på. Kommunen behandler store mengder sensitive personopplysninger, og det må forventes stor aktpågivenhet ved behandling av personopplysninger av denne karakter.

Vi mener at Årdal kommune i tillegg må iverksette organisatoriske og/eller tekniske sikkerhetstiltak for å gjøre det vanskeligere for en ansatt å gi feil tilgang til et dokument ved webpublisering.

Konklusjon: Årdal kommune må iverksette organisatoriske og/eller tekniske sikkerhetstiltak for å begrense muligheten for at uautorisert publisering av dokumenter på Internett, i samsvar med personopplysningsloven § 13, jf. personopplysningsforskriften §§ 2-1, 2-2, 2-11 og 2-14.

Risikovurdering
Forskriftens § 2-4 andre ledd krever at den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for, og konsekvenser av, sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

Datatilsynet mener at publisering av fulltekstdokumentasjon på Internett er en behandling av personopplysninger med sannsynlighet for avvik og hvor konsekvensen kan være svært alvorlig for de som rammes av dette. Dette er følgelig en behandling som krever risikovurdering.

Datatilsynet mottok kommunens gjeldende rutiner og risikovurderinger i brev av 15. mars 2016. I oversendelsen fremgår det at det ikke har vært gjennomført egen risikovurdering knyttet til innføring av ny praksis med postjournal på nett på slutten av 1990-tallet, og heller ikke da rutinene ble oppdatert i tilknytning med vedtak om nytt informasjonsreglement i 2010.

Konklusjon: Det konstateres at det ikke har vært gjennomført egen risikovurdering for publisering av personopplysninger på Internett.

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 Årdal kommune har behandlet sensitive personopplysninger på en måte som er i strid med lov, jf personopplysningsloven § 11 bokstav a (manglende rettslig grunnlag, § 13 (mangelfull informasjonssikkerhet) og § 14 (mangelfull internkontroll).

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 også vekt på alvoret i at det ikke var adgang til å publisere sensitive personopplysninger etter personopplysningsloven § 11 bokstav a, jf. §§ 8 og 9, selv om dette ikke var tilsiktet. Brukerne av kommunens 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.

Datatilsynet legger videre vekt på at det er noe å bebreide Årdal kommune når det gjelder det som har skjedd jf. § 46 annet ledd bokstav b. For å opprettholde tillitsforholdet mellom forvaltning og borgere er forventningen at Årdal kommune setter seg grundig inn i personopplysningsregelverket og etablerer gode rutiner for å sikre etterlevelsen av det. I skjerpende retning legger Datatilsynet til grunn at publiseringen av sensitive personopplysninger berører en gruppe mennesker (psykisk utviklingshemmede) som trenger særskilt beskyttelse da de i liten grad kan ivareta sine rettigheter selv.

Det finnes dessuten mye veiledning utarbeidet for utøvelsen av offentlighet og meroffentlighet. Hendelser knyttet til publisering av sensitive personopplysninger via publiseringsløsninger for postlister har dessuten i en årrekke vært omtalt i media. Årdal kommune må ha vært klar over risikoen ved å legge opp til at fulltekstdokumentasjon skal være tilgjengelig via Internett.

I skjerpende retning legges også vekt på at kommunen ikke har risikovurdert behandlingen av personopplysninger ved publisering på Internett, slik forskriften § 2-4 forutsetter. At kommunen har utarbeidet rutiner for meroffentlighet er ikke tilstrekkelig i forhold til forskriften § 2-4. En gjennomført risikovurdering ville ha satt kommunen i stand til å se sannsynligheten for en hendelse og konsekvensen av den. Manglende risikovurdering har også som følge at det ikke er blitt utarbeidet kriterier for akseptabel risiko forbundet med behandlingen av personopplysningene.

Årdal kommune har heller ikke iverksatt tekniske tiltak som kunne ha forebygget overtredelsen, f.eks. ved tekniske sperrer fra sikker sone. Dette kan gjøres på forskjellige måter, men Datatilsynet kan ikke se at dette har vært vurdert av kommunen. Det kan ikke

statueres gjentakelse direkte i og med at dette er første gang dette påpekes overfor kommunen, jf. § 46, fjerde ledd bokstav f.

Kommunen hadde etablerte organisatoriske sikkerhetstiltak knyttet til prosessen med oversendelse av personsensitive opplysninger fra Gerica via ACOS og BEST til Fylkesmannen. Avviket skyldes menneskelig svikt. Det er på det rene at hvis rutinene var blitt fulgt ville ikke dette avviket oppstått.

Datatilsynet er kjent med at det opprinnelig ble reist erstatningssøksmål mot kommunen fra de berørte i denne saken. Vi har imidlertid forstått det slik at partene er kommet til en minnelig løsning hvor kommunen utbetaler et beløp til hver av de berørte familiene for tort og svie. Dette er et moment som kan tale i retning av å ikke ilegge overtredelsesgebyr.
Sett opp mot øvrige momenter i saken kan imidlertid ikke Datatilsynet se at kommunens utbetaling av et mindre beløp til den enkelte tilsier at gebyr ikke bør ilegges. Formålet med erstatning for tort og svie dekker et annet formål enn reaksjonen fra tilsynsmyndigheten. Vi har derfor i liten grad lagt vekt på dette faktum i vurderingen av om gebyr skal ilegges. Det at dem saken gjelder føler at de har krav på erstatning kan også sees på som et utrykk for en opplevd krenkelse, og som et utrykk for en personvernkonsekvens av kommunens håndtering av opplysninger om de.

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

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

Konklusjon
Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges.

Gebyrets størrelse
Når det gjelder gebyrets størrelse, skal de samme momenter 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.

Det er særlig sett hen til at dette avviket omfatter svært sensitive personopplysning om en gruppe mennesker (psykisk utviklingshemmede) som i liten grad kan ivareta sine rettigheter. Dette taler for en streng reaksjon. Videre har vi sett på den generelle forventning borgerne skal kunne ha til at kommunale instanser følger de regler som er gitt, og særlig de som gir enkeltindivider rettigheter som er ment å være en beskyttelse mot utlevering av denne typen opplysninger. Det er ikke tvilsomt at opplysningene er taushetsbelagte, og kommunen burde hatt laget bedre systemer for å sikre så sensitiv informasjon.

Signalvirkningen av denne saken, de allmennpreventive hensyn, mener vi er tydelige i denne saken. Vi ønsker å tydeliggjøre at slike hendelser ikke må skje og at alle offentlige instanser som behandler sensitive personopplysninger må være seg sitt ansvar bevisst.

Mangelfulle rutiner har ofte som konsekvens at risikoen for feil øker. I denne saken har svake rutiner faktisk hatt en reell konsekvens som også tilsier en skjerpet reaksjon.

I sitt tilsvar påpeker kommunen at det ikke er tatt nødvendig hensyn til at avviket skyldes en personlig feil fra en ansatt, og at man aldri kan gardere seg fullt ut mot at dette skal skje i framtiden. Datatilsynet deler dette synspunktet, men er av den oppfatning at kommunen ikke har gjort nok for å minimalisere at slike hendelser kan skje.

Datatilsynet har vurdert varslet overtredelsesgebyr på nytt og kommet til at det er satt noe høyt. Kommunen hadde etablerte organisatoriske sikkerhetstiltak knyttet til prosessen med oversendelse av personsensitive opplysninger fra Gerica via ACOS og BEST til Fylkesmannen. Avviket skyldes menneskelig svikt. Det er på det rene at hvis rutinene var blitt fulgt ville ikke dette avviket oppstått.

Etter en totalvurdering av saken og da særlig sett hen til alvorligheten i overtredelsen har vi kommet til at et overtredelsesgebyr på 150.000 anses riktig.

Frist for gjennomføring av påleggene

Datatilsynet gir frist for gjennomføring av pålegget(ene) til **1. september 2016.** Kommunen må innen nevnte dato bekrefte skriftlig overfor Datatilsynet at pålegget(ene) er gjennomført. Med mindre annet er særskilt angitt kreves det ikke ytterligere dokumentasjon på at pålegget er gjennomført. Det gjøres imidlertid oppmerksom på at Datatilsynet vil kunne foreta en etterkontroll av dette.

Klageadgang

Dette vedtaket kan påklages i henhold til forvaltningslovens bestemmelser. Eventuell klage må fremsettes overfor Datatilsynet **innen tre uker** etter at vedtaket ble mottatt. En eventuell klage oversendes Personvernnemnda for klagebehandling. Datatilsynet gjør i den forbindelse oppmerksom på retten til innsyn i sakens dokumenter, jf. forvaltningsloven § 18.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Kaspersen
fagdirektør