

Askvoll kommune
Postboks 174
6988 ASKVOLL

Deres referanse

Vår referanse
16/00364-4/KBK

Dato
16.06.2016

Vedtak om overtredelsesgebyr - Publisering av personopplysninger i personalsak - Askvoll kommune

Det vises til varsel om overtredelsesgebyr av 8. april 2016. Datatilsynet har ikke mottatt svar på varslet, og legger derfor til grunn varslet vedtak.

18. februar 2016 varslet Askvoll kommune at de hadde hatt et avvik hvor et dokument med informasjon om en alvorlig personalsak med lett identifiserbare personer ble lagt ut på kommunen sin sakliste i møteportal for politisk utvalg, her Arbeidsmiljøutvalget, og gjort tilgjengelig på Internett.

Sakens faktiske forhold

Askvoll kommune har publisert et saksdokument i en alvorlig personalsak på Internett (hjemmesiden til kommunen). Det framgår ikke navn på angjeldende person i dokumentet, men vedkommende er identifisert med stillingsbeskrivelse. I dokumentet, som ble publisert, skisseres to mulige løsninger; å opprette en retrettsstilling, eller om vedkommende skal sies opp. Dette lå som en vurdering fra rådmannen. Dokumentet var en kladd, og var ikke det endelige dokument som ble lagt fram for Arbeidsmiljøutvalget.

Askvoll kommune ved rådmannen ble varslet av en journalist i Firda om at saksdokumentet var publisert på nett.

Iht. avviksmeldingen skjedde følgende med dokumentet:

Saksnotatet ble registrert til «U3 – unntatt offentlighet» før oppstart. Dokumentet ble så sendt til rådmannen som flaggmelding for uttalelse. Saken ble sendt tilbake fra rådmannen med merknad «utan uttale». Dokumentet var skrivebeskyttet, noe som medførte at det ikke kunne endres i tråd med rådmannens ønsker. Sammen med arkivleder prøvde saksbehandler (personalsjef) å åpne dokumentet uten hell. For å få endret dokumentet opprettet arkivleder versjon 2 av dokumentet. Hele mappen ble overført til personalmappen og dobbeltsjekket for at alt var avkrysset for U3. Deretter ble dokumentet sendt til AMU for saksbehandling. Dette dokumentet ble ikke publisert på nettet. Det er dokumentet som kom fra rådmannen (versjon 1 – kladdeversjonen)) som ble publisert på nettet.

Etter at avviket ble oppdaget har kommunen i samarbeidet med leverandør og andre kommuner i Sunnfjord og Ytre Sogn IKT-nettverket arbeidet for å finne ut hva som har skjedd. Kommunen føler at leverandør fraskriver seg sitt informasjons- og opplæringsansvar ved innføring av ny modul i saksarkivet.

Nærmere detaljer om avviket framgår av avviksmeldingen av 18. februar 2016.

Datatilsynet har merket seg at kommunen har et avvikhåndteringssystem som vi vurderer som bra med de kriterier det inneholder.

Varsel om overtredelsesgebyr

Askvoll kommune pålegges i medhold av personopplysningsloven § 46, første ledd, jf. §§ 11 a og 13 å betale et overtredelsesgebyr til statskassen, stort kroner **75.000 – syttifemtusen**, for å ha behandlet personopplysninger uten behandlingsgrunnlag jf. § 11 a, og uten å etablere tilfredsstillende tiltak for å hindre uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig, jf. forskriften § 2-11, og for ikke å ha sikret at medarbeiderne har kompetanse til å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt, jf. forskriften § 2-8.

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

Nærmere om internkontrollplikten - generelt

Et viktig formål bak personopplysningsloven er å ansvarliggjøre virksomheter når det gjelder 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, utfra 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, bl.a. 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 de 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, og inneholdt svært alvorlige forhold på arbeidsplassen. Dette er innenfor personopplysningslovens anvendelsesområde.

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. personopplysningslovens forskrifter § 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 for å kunne publisere taushetsbelagte personopplysninger på Internett. I dette tilfellet er opplysningene ikke sensitive etter personopplysningsloven, se § 2 nr. 8.

Offentleglova § 10 og offentlegforskrifta § 7 fastslår at taushetsbelagte personopplysninger 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).

Konklusjon:

Askvoll kommunes publisering av taushetsbelagte personopplysninger på Internett mangler behandlingsgrunnlag etter personopplysningsloven § 11 a) jf. § 8.

Rutinene for opplæring av ansatte

Askvoll kommunen har vedtak om å praktisere meroffentlighet, noe som betyr at kommunen i størst mulig grad skal legge til rette for offentlighet og innsyn i kommunen sine saksdokumenter. Det er da viktig at det er utarbeidet gode rutiner for publisering av postliste med lenker på nett, og at ansatte får den opplæring som er nødvendig for å kunne bruke

systemet. Kommunen er av den oppfatning at de ikke har fått den nødvendige kunnskap som kunne gjøre dem i stand til å hindre dette avviket; og peker på at dette er Acos (leverandør) sitt ansvar. Datatilsynet tar ikke stilling til hvorvidt Acos har gitt tilstrekkelig informasjon om systemet, men påpeker at det er den behandlingsansvarlige som har ansvar for at de ansatte får den nødvendige kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er lagt, jf. forskriften § 2-8. Slik avviket er beskrevet er det klart at de ansatte ikke har fått nødvendig opplæring i systemet, og således ikke skulle tatt dette i bruk før dette var på plass.

Konklusjon: De ansatte har ikke fått nødvendig kunnskap for å kunne bruke informasjonssystemet i samsvar på de rutiner som er lagt, jf. forskriften § 2-8.

Datatilsynets vurdering av overtredelsesgebyr

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

Datatilsynet kan pålegge den som har overtrødt 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 forsettlig eller uaktsomme overtrødelser. Et foretak kan ikke ilegges overtredelsesgebyr dersom overtrødelsen skyldes forhold utenfor foretakets kontroll.

Ved vurderingen av om overtredelsesgebyr skal ilegges, og ved utmålingen, skal det særlig legges vekt på

- a) hvor alvorlig overtrødelsen har krenket de interesser loven verner,*
- b) graden av skyld,*
- c) om overtrøderen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtrødelsen,*
- d) om overtrødelsen er begått for å fremme overtrøderens interesser,*
- e) om overtrøderen har hatt eller kunne ha oppnådd fordel ved overtrødelsen,*
- f) om det foreligger gjentakelse,*
- g) om andre reaksjoner som følge av overtrødelsen blir ilagt overtrøderen eller noen andre som har handlet på vegne av denne, blant annet om noen enkeltperson blir ilagt straff og*
- h) overtrøderens 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 lovovertrødelse for å kunne ilegge gebyr. Saksforholdet og spørsmålet om å ilegge overtredelsesgebyr er vurdert med utgangspunkt i dette beviskravet.

Datatilsynet finner det klart at Askvoll kommune har behandlet sensitive personopplysninger på en måte som er i strid med lov, jf. personopplysningsloven § 11 bokstav a (manglende rettslig grunnlag og § 13 (mangelfull informasjonssikkerhet).

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 særlig vekt på alvoret i at det ikke var adgang til å publisere taushetsbelagte personopplysninger etter personopplysningsloven § 11 bokstav a, jf. § 8. Brukerne av kommunens tjenester har en klar beskyttelsesverdig interesse mot ulovlig publisering av konfidensielle opplysninger. Dette gjelder også for kommunens egne ansatte. 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.

I skjerpene retning legges det vekt på at kommunen ikke har gitt sine ansatte nødvendig oppløring for å kunne bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.

Datatilsynet legger videre vekt på at det er noe å bebreide Askvoll kommune når det gjelder det som har skjedd, jf. § 46 annet ledd bokstav b. Kommunen behandler store mengder taushetsbelagte personopplysninger i sin virksomhet. For å opprettholde tillitsforholdet mellom forvaltning og borgere/ansatte er forventningen at Askvoll kommune setter seg grundig inn i personopplysningsregelverket og etablerer gode rutiner for å sikre etterlevelsen av det.

Det er kommunens ansvar å forsikre seg om at brukere av systemet, som de måtte forstå publiserte opplysninger på nett, faktisk hadde nødvendig kunnskap, og at systemet ikke ble implementert før dette var på plass.

Det finnes dessuten mye veiledning utarbeidet for utøvelsen av offentlighet og meroffentlighet. Hendelser knyttet til publisering av taushetsbelagte personopplysninger via publiseringsløsninger for postlister har dessuten i en årrekke vært omtalt i media.

Askvoll 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 hos kommunen. Det kan ikke statueres gjentagelse direkte i og med at dette er første gang dette påpekes overfor kommunen, jf. § 46, fjerde ledd bokstav f.

Gjennom bedre internkontroll i form av skriftlige rutiner for kvalitetssikring av gradering av dokumenter og linker til dokumenter kunne overtredelsene vært unngått, jf. § 46 annet ledd bokstav c. Internkontroll er en nødvendig forutsetning for at den behandlingsansvarlige skal kunne forsikre seg om, og løpende kontrollere at virksomheten til enhver tid følger personopplysningslovens bestemmelser.

Datatilsynet har tidligere ilagt overtredelsesgebyr for manglende interkontroll hos offentlige aktører bl.a. kommuner. I denne saken har svakheter i interne rutiner faktisk hatt som konsekvens at ikke offentlige opplysninger har blitt eksponert. Det er et sterkt argument for at gebyr skal ilegges.

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 i nevneverdig grad – verken i skjerpene 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 en generell forventning at kommunale institusjoner følger de regler som er gitt og særlig når det gjelder regler som gir enkeltindivider rettigheter som er ment å være et beskyttelsesmekanisme mot overgrep fra kommunale institusjoner.

Etter en vurdering av alvorligheten i overtredelsen har vi kommet til at et overtredelsesgebyr på 75.000 anses passende.

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 Personvernemnda 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