Datatilsynet

Harstad kommune
c/o Postmottak,
Postboks 1000
9479 HARSTAD

Deres referanse	Vår referanse	Dato
2016/143 / 041	16/00061-6/EOL	17.06.2016

Vedtak om overtredelsesgebyr - Harstad kommune - Publisering av sensitive personopplysninger på Internett

Vi viser til varsel om pålegg og overtredelsesgebyr for publisering av sensitive personopplysninger på internett av 8. april 2016. I tilbakemelding av 26. april 2016 skriver Harstad kommune at varselet inneholder en korrekt saksfremstilling.

Vurdering av tilsvar
Datatilsynet mottok deres kommentarer til vårt varslede vedtak i brev av 26. april 2016. Vi har følgende kommentarer til det som fremkommer av deres gjennomgang av pålegg:

Varslet pålegg 1 – Iverksetting av tekniske tiltak for å hindre publisering av konfidensielle personopplysninger
Harstad kommunehar endret standardverdi fra «Ja» til «Nei» med hensyn til automatisk publisering av dokumenter uten tilgangskode i innsynsløsningen sin. Dette betyr at alle dokumenter manuelt må markeres for å publiseres. I tillegg har kommunen innført en rutine for kvalitetssjekk av dokumenter ved at alle dokumenter skal gjennomgåes av to forskjellige personer før de publiseres. Avvikspunktet anses lukket.

Varslet pålegg 2 – Informasjon til partene i sakspapirene
Harstad kommuneerklærer at alle berørte i saken er informert. Datatilsynet legger kommunens erklæring til grunn, og anser avvikspunktet for lukket.

Varslet overtredelsesgebyr
Harstad kommune argumenterer for at rask opprydding, erkjennelse av ansvar og forandring av rutiner for fremtiden bør tilsi at gebyrets størrelse kan reduseres.

Vurderingen av hvorvidt overtredelsesgebyr skal ilegges er basert på tilstanden da avviket skjedde. Etterfølgende korrigerende tiltak er følgelig ikke relevante for denne vurderingen. Ved utmåling av overtredelsesgebyr skal det legges vekt på de samme momentene som ved vurderingen av om det skal ilegges overtredelsesgebyr. Det er følgelig heller ikke her adgang til å vektlegge korrigerende tiltak som er gjennomført etter hendelsen som utløste pålegg om overtredelsesgebyr. At kommunen endrer rutinene viser at den tidligere tilstanden var en for

usikker rutine og underbygger tilsynets konklusjon mer enn den er egnet til å påvirke utmålingen av overtredelsesgebyr.

Vedtak om overtredelsesgebyr

Datatilsynet fatter med hjemmel i personopplysningsloven § 46 følgende vedtak:

> *Harstad kommune pålegges å betale til statskassen et overtredelsesgebyr pålydende 100.000 - etthundretusen – kroner for uautorisert utlevering av konfidensielle personopplysninger på internett i strid med personopplysningsloven § 11 a, jf. § 8.*

Oppfyllelsesfristen er 4 uker etter at vedtaket om overtredelsesgebyr er endelig.
Vedtaket er tvangsgrunnlag for utlegg, jf. personopplysningsloven § 47 a.

Inndrivelse av kravet vil bli overlatt til Statens innkrevingssentral.

Begrunnelsen for vedtaket
Datatilsynet legger til grunn følgende:

Harstad kommune mottok 04.01.16 en e-post som inneholdt sensitive personopplysninger. E-posten ble registrert uten tilgangskode, det vi si at det ikke ble lagt inn noen begrensninger for eventuell publisering i journalsystemet. Journalføringen førte til at dokumentet ble publisert ved at e-posten var tilgjengelig på internett. At dette dokumentet lå offentlig tilgjengelig ble oppdaget av en journalist i Harstad Tidende. Journalisten varslet saksbehandler i kommunen, og dokumentet ble da gradert og fjernet fra innsynsløsningen. Dette skjedde 1 døgn etter at det ble tilgjengeliggjort.

Følgende opplysninger fremkommer av e-posten:

- Avsenders navn
- Familiemedlemmers diagnoser

Kommunen påpekte at navn på familiemedlemmer ikke fremkom direkte av e-posten. Når kommunen benevner disse personene som «familiemedlemmer» så går vi ut fra at e-postens innhold avslører relasjonen mellom avsender og de som er omtalt i e-posten. Datatilsynet legger til grunn at kombinasjonen navn på avsender og opplysning om familierelasjon er tilstrekkelig til å identifisere personene som er omtalt. Når de konkrete opplysningene som fremgår er diagnoser legger vi til grunn at e-posten som kommunen mottok inneholdt taushetsbelagte opplysninger og skulle vært unntatt offentlighet med hjemmel i offentleglova § 13 første ledd. Brevet inneholdt videre personopplysninger som er å anse som sensitive, jf. personopplysningsloven § 2 nr. 8.

Konsekvensen av avviket var at dokumentet som fremgikk av postlista var tilgjengelig i klartekst via en lenke, og sensitive personopplysninger lå tilgjengelig i 1 døgn før det ble oppdaget av en ekstern part.

Harstad kommune erklærte opprinnelig at det var igangsatt skjerpet kontroll av registrert post og postliste. Etter pålegg fra Datatilsynet er det nå også innført tekniske tiltak for å unngå publisering av sensitive personopplysninger for fremtiden.
De personer som hadde fått sine sensitive personopplysninger utlevert var opprinnelig ikke informert om avviket. Etter pålegg fra Datatilsynet skal nå Harstad kommune ha varslet alle berørte om avviket.

Nærmere om internkontrollplikten - generelt
Et viktig formål med 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 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 både underlagt taushetsplikt og inneholdt sensitive personopplysninger (diagnose).

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:
Harstad kommunes publisering av sensitive personopplysninger på internett mangler behandlingsgrunnlag etter personopplysningsloven §§ 8 og 9.

Rutinene for publisering av personopplysninger på nett
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.

Harstad kommune har beskrevet at de har iverksatt organisatoriske tiltak, slik som gjennomgang av rutiner og opplæring, men dette har ikke vært tilstrekkelig for å hindre at konfidensielle opplysninger ble publisert. Etter Datatilsynets vurdering er tiltakene som er planlagt for å kvalitetssikre publisering av offentlig postliste på papir og nett for generelle. Det er kontrollen av hvorvidt et dokument inneholder sensitive personopplysninger som har sviktet. I tillegg er det ikke gjort noen kontroll av om dokumentet kunne publiseres da det ble linket til fulltekstdokumentet fra postlisten. Kommunens rutiner 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.

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, legger derfor Datatilsynet 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 Harstad 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 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 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 sterkt virkemiddel som overtredelsesgebyr.

I skjerpende retning legger Datatilsynet til grunn at publiseringen av sensitive personopplysninger gjelder diagnoser, som er opplysninger som det ellers er strenge konfidensialitetskrav rundt. Dette er også en kategori opplysninger som den enkelte normalt ønsker å ha kontroll på med hensyn til hvem som har tilgang til.

Dokumentet var tilgjengelig på internett i 1 døgn. Dette er relativt kort tid og kan være et moment i formildende retning.

Datatilsynet legger vekt på at Harstad kommune er å bebreide for overtredelsene, jf. § 46 annet ledd bokstav b. For å opprettholde tillitsforholdet mellom forvaltning og borgere er forventningen at Harstad kommune setter seg grundig inn i personopplysningsregelverket og etablerer gode rutiner for å sikre etterlevelsen av det.

Det finnes 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. Harstad kommune må ha vært klar over risikoen ved å legge opp til at fulltekstdokumentasjon skal være tilgjengelig via internett. Når det i tillegg er et uttrykkelig forbud mot slik publisering i offentleglova § 10 tredje ledd, jf. offentlegforskriften § 7 første ledd bokstav a og c mener vi dette underbygger at Harstad kommune er å bebreide for den urettmessige publiseringen.

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

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 skjerpende eller formildende retning.

Sett opp mot øvrige momenter i saken kan ikke Datatilsynet se at det faktum at opplysningene var tilgjengelige i relativt kort tid tilsier at gebyr ikke bør ilegges. At publiseringstiden ble kort må anses som tilfeldig da det ikke var Harstad kommune selv som oppdaget avviket, men måtte bli varslet av en ekstern part. Heller ikke det moment at det ikke er konstatert gjentagelse er tungtveiende nok til å tilsi at gebyr ikke bør ilegges. Datatilsynet har en annen sak til behandling[1] som i likhet med denne tyder på at Harstad kommune ikke har rutiner som er egnet til å forhindre at taushetsbelagte og beskyttelsesverdige opplysninger blir publisert på innsynsløsningen for postjournal. Samlet sett taler momentene over for at gebyr bør ilegges.

[1] 16/00550

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 sensitive personopplysning som diagnoser. Dette taler for en streng reaksjon. Videre har vi sett på den generelle forventning borgerne skal kunne ha til at kommunale institusjoner 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 sensitiv informasjon.

Samtidig er det et faktum at opplysningene var tilgjengelige i relativt kort tid. Dette er noe som taler for at beløpet ikke bør være i det øvre sjiktet av det som er mulig å gi, og som vi har tillagt større vekt enn i varslet vedtak.

Signalvirkningen av denne saken, de allmennpreventive hensyn, mener vi imidlertid er tydelige i denne saken. Vi ønsker å tydeliggjøre at slike hendelser ikke må skje og at alle offentlige instanser som har 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.

Vi opprettholder at et beløp på NOK 100.000,- er en passende reaksjon.

Klageadgang
Vedtak om overtredelsesgebyr er et enkeltvedtak som kan påklages til Personvernnemnda, jf. personopplysningsloven § 42 siste ledd.

Frist for å klage er **3 uker** fra vedtaket ble mottatt. Eventuell klage fremsettes til Datatilsynet.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver