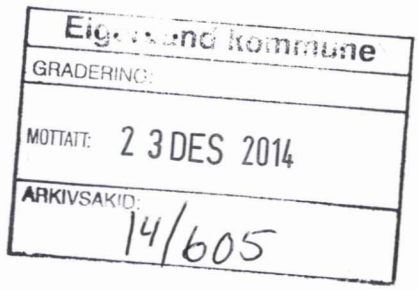
Datatilsynet



Eigersund kommune
v/rådmannen

4370 EGERSUND

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	14/00406-2/KBK	18. desember 2014

Varsel om vedtak om pålegg og overtredelsesgebyr - Foreløpig kontrollrapport for Eigersund kommune - Internkontroll og informasjonssikkerhet

Den 30. april 2014 gjennomførte Datatilsynet en kontroll hos **Eigersund kommune**. Kontrollen skjedde med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 42 tredje ledd nr. 3.

Foreløpig kontrollrapport
De avvik som ble avdekket i kontrollen er nærmere beskrevet i vedlagte kontrollrapport. Eventuelle feil eller mangler i de faktiske forhold som fremkommer i rapporten bes tatt opp med Datatilsynet i forbindelse med virksomhetens eventuelle tilsvar til dette varselet, jf siste avsnitt i dette brev. Det gjøres i den forbindelse oppmerksom på at rapporten skal gjenspeile de faktiske forhold på kontrolltidspunktet, slik at eventuelle senere endringer ikke får betydning for rapportens innhold. Dersom Datatilsynet ikke mottar merknader til kontrollrapporten blir denne å anse som endelig ved fristens utløp.

Alle henvisninger til lovhjemler i kontrollrapporten er knyttet til personopplysningsloven og dens forskrifter. Andre henvisninger til lovhjemler er nevnt særskilt.

Datatilsynet ønsker innledningsvis å påpeke at det er alvorlig at en offentlig virksomhet ikke følger de lover og regler som er pålagt dem. Gjennom kontrollen ble det opplyst at manglende prioritering var årsaken til at det ikke var laget dokumenterte rutiner for etterlevelse av personopplysningsloven. Dette finner Datatilsynet urovekkende.

Varsel om vedtak
Dette er et varsel etter forvaltningsloven § 16 om at Datatilsynet vil fatte følgende vedtak:

1. Eigersund kommune pålegges i medhold av personopplysningsloven§ 46, fjerde ledd, jf. § 14, jf. personopplysningsforskriften § 3-1 å etablere og holde ved like systematiske tiltak som er nødvendige for å oppfylle kravene i personopplysningsloven (internkontroll) og dokumentere tiltakene, blant annet:
    a) rutiner for ivaretakelse av enhvers (borgerens) krav om innsyn i kommunens behandlinger, jf. § 18 første ledd, og den registrertes rett til innsyn i egne

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

opplysninger etter § 18 andre ledd, jf. § 14 og forskriften § 3-1 tredje ledd bokstav d). Se kontrollrapportens pkt. 6.1.4.1.

b) rutiner for ivaretakelse av den registrertes rett til informasjon etter §§ 19 og 20, jf. § 14 jf. forskriften § 3-1 tredje ledd bokstav d). Se kontrollrapportens 6.1.4. 2.

c) rutiner for retting og sletting, i samsvar med §§ 27 og 28, jf. § 14 jf. forskriften § 3-1 tredje ledd bokstav c). Se kontrollrapportens pkt. 6.1.4.3.

d) rutiner for oppfyllelse av personopplysningslovens regler om melde- og konsesjonsplikt etter §§ 31-33, jf. § 14 jf. forskriften § 3-1 tredje ledd bokstav f). Se kontrollrapportens pkt. 6.1.4.4.

2. Kommunen pålegges i medhold av personopplysningsloven § 46, fjerde ledd, jf. § 13 å etablere tilfredsstillende informasjonssikkerhet, herunder

   a. i henhold til forskriften § 2-4 første ledd å utarbeide en oversikt over behandlinger av personopplysninger som viser hvilke personopplysninger som behandles, formålet med behandlingen og lovgrunnlaget. Det vises til kontrollrapportens pkt. 6.1.3.

   b. i henhold til. forskriften § 2-3 å danne rammer for sikkerhetsarbeidet ved at det etableres sikkerhetsmål og –strategi. Det vises til kontrollrapportens pkt. 6.2.1.

   c. i henhold til forskriften § 2-7 å etablere et behandlingsansvar som synliggjøres i organisasjonen. Se kontrollrapportens pkt. 6.1.2.

   d. i henhold til forskriften § 2-7 å dokumentere sikkerhetsorganisasjonen. Se kontrollrapportens pkt. 6.2.1.

   e. i henhold til forskriften §§ 2-4 og 2-15 å gjennomføre risikovurdering for all behandling av personopplysninger. Se kontrollrapportens pkt. 6.2.2.

   f. i henhold til forskriften §§ 2-5 å etablere rutiner for sikkerhetsrevisjon. Se kontrollrapportens pkt. 6.2.3.

   g. i henhold til forskriften §§ 2-11, 2-12, 2-13 og 2-14 å innføre og dokumentere sikkerhetstiltak. Se kontrollrapportens pkt. 6.2.5.

   h. i henhold til forskriften § 2-8 å etablere rutiner for og gjennomføre opplæring av ansatte for sikker bruk av informasjonssystemet. Se kontrollrapportens pkt. 6.2.6.

   i. i henhold til §§ 15 og 13 jf. forskriften §§ 2-15 å etablere og oppdatere avtaler med sine databehandlere slik at de oppfyller kravene til en databehandleravtale. Se kontrollrapportens pkt. 6.3.

Varsel om overtredelsesgebyr

Dette er et varsel etter forvaltningsloven § 16 om at Datatilsynet vil fatte følgende vedtak:

1. Eigersund kommune pålegges i medhold av personopplysningslovens § 46, første ledd, jf. §§ 13 og 14 å betale et overtredelsesgebyr til statskassen, stort kroner **250.000 – tohundreogfemtitusen**, for å ha behandlet personopplysninger uten å ha etablert dokumenterte tilfredsstillende tiltak for å sikre at behandlingen skjer i tråd med

personopplysningslovens bestemmelser (internkontroll) og uten å ha sørget for tilfredsstillende informasjonssikkerhet ved behandlingen.

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
Personopplysningsloven har blant annet som formål å ansvarliggjøre virksomheter for dets 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 forskriften § 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 dokumentert og implementert, slik at de i praksis ligger til grunn for virksomhetens behandling av personopplysninger.

Datatilsynet vurdering av overtredelsesgebyr
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.

Ved vurderingen om det skal ilegges et overtredelsgebyr er det lagt vekt på at 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 mener unnlatelsen av å etablere internkontroll og derigjennom manglende dokumenterte rutiner er et betydelig avvik og må ansees alvorlig i forhold til de interesser loven verner, jfr. § 46, andre ledd bokstav a).

Forventningen om at en kommune setter seg grundig inn i personopplysningsregelverket og etablerer gode rutiner for å sikre etterlevelsen av det har betydning for vurderingen av skyldgraden etter § 46, andre ledd bokstav b). Det kan her vises til at Eigersund kommune behandler sensitive personopplysninger i store deler av sin virksomhet. At de på kontrolltidspunktet ikke kunne vise at de hadde rutiner for dette vektlegger vi i skjerpende

retning, både når det gjelder vurderingen av om gebyr skal ilegges og ved utmåling av størrelsen.

Datatilsynet har også lagt vekt på at mangelfull internkontroll og lovstridig praksis kan ha konsekvenser for de registrerte. Kontrollen avdekker også at det ikke er foretatt noen risikovurdering i henhold til forskriften § 2-4. Flere systemer i kommunen er ikke under IT-avdelingens kontroll. Disse administreres av superbrukere. Det er bekymringsfullt at kommunen ikke har nødvendig kontroll på disse systemene. I tillegg var en overordnet ROS-analyse for beredskap i oktober 2013 kritisk til mangelen på risikovurderinger for informasjonssikkerheten. Det gjør at kommunen i liten grad er i stand til å forutse potensielle konsekvenser for personvernet og andre sikkerhetshendelser som omfatter personopplysninger. Plikten etter denne bestemmelsen er også et uttrykk for interesser loven verner, og brudd på plikten er et argument for ileggelse av overtredelsesgebyr, jf § 46, 1. ledd, bokstav a)

Det kan ikke statueres gjentakelse direkte i og med at dette er første gang dette påpekes overfor kommunen, jf. § 46, fjerde ledd bokstav f), men at forholdet har vart i mange år vurderes som skjerpende i relasjon til graden av skyld, jf bokstav b).

Manglene er av en slik art og omfang at det medfører etter vår oppfatning en uholdbar risiko for at kommunen i praksis bryter andre helt sentrale bestemmelser i personopplysningsloven, uten at dette kan oppdages av virksomheten selv eller tilsynsmyndigheten. Mangelen er av den grunn også skjerpende i vurderingen av om overtredelsesgebyr skal ilegges jf. § 46, andre ledd bokstav c) hvor det skal vektlegges om retningslinjer m.v. kunne forebygget overtredelsen.

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

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.

Tilnærmet totalt fravær av et internkontrollsystem karakteriseres som et alvorlig avvik og taler for en streng reaksjon. At det er snakk om en kommunal myndighet mener vi også er et argument i samme retning. Det er en generell forventning at statlige institusjoner følger de regler som er gitt og særlig når det gjelder regler som gir enkeltindivider rettigheter som er ment å være en beskyttelsesmekanisme mot overgrep fra statlige institusjoner.

Det er i denne saken, som nevnt over, vanskelig å vurdere om kommunen har rutiner som er egnet til å ivareta personvernet til de som er registrert på grunn av manglende dokumenterbare rutiner.

Datatilsynet har gjennom flere kontroller erfart at statlige og kommunale institusjoner har store mangler i sine plikter til å ha internkontrollsystem. Ileggelsen av overtredelsesgebyr vil derfor ha en allmennpreventiv hensikt. Det er viktig at etater og institusjoner som håndterer opplysninger om befolkningen har gode systemer internt som sikrer at de tildelte rettigheter som borgerne har ikke blir neglisjert.

Etter en vurdering av alvorligheten i overtredelsen har vi komme til at et overtredelsesgebyr på 250.000 anses passende. Dette samsvarer også med pålegg som er gitt andre offentlige etater, hvor rutiner for internkontroll og informasjonssikkerhet har vært sterkt mangelfulle eller helt fraværende.

Tilsvar
Eventuelle merknader til foreliggende varsel eller kontrollrapport bes sendt Datatilsynet snarest, og senest **innen fredag 30. januar 2015.** Det anbefales at virksomheten oversender Datatilsynet et forslag til fremdriftsplan for lukking av de avvik som er beskrevet i kontrollrapporten. Datatilsynet vil se hen til denne fremdriftsplanen når det skal vedtas en frist for virksomhetens gjennomføring av vedtaket.

Med vennlig hilsen

Bjørn Erik Thon
Direktør

Knut-Brede Kaspersen
fagdirektør

Vedlegg: Foreløpig kontrollrapport