Datatilsynet

Foreløpig kontrollrapport		
Saksnummer: 14/00406 Dato for kontroll: 30.04.2014 Rapportdato: ~~01.09.2014~~18.12.2014	Kontrollobjekt: Eigersund kommune Sted: Egersund	Utarbeidet av: Knut-Brede Kaspersen Ted Tøraasen

1 Innledning

Datatilsynet gjennomførte kontroll hos **Eigersund kommune** 30. april 2014. Kontrollen ble utført med hjemmel i personopplysningsloven § 44, jf. § 42, 3. ledd.

Temaet for kontrollen var virksomhetens behandling av personopplysninger, særlig i forbindelse med plikt til å innføre internkontroll og å sørge for tilfredsstillende informasjonssikkerhet i henhold til gjeldene lover og forskrifter. Kontrollen ble gjennomført på virksomhetens faste besøksadresse.

I det følgende vil Datatilsynet beskrive de faktiske forhold som ble avdekket under kontrollen. Kontrollrapporten danner grunnlag for Datatilsynets vurderinger og eventuelle pålegg. Alle henvisninger til lovhjemler i kontrollrapporten er knyttet til personopplysningsloven og dens forskrifter. Andre henvisninger til lovhjemler er nevnt særskilt.

2 Tilstede under kontrollen

2.1 Fra virksomheten:

- Morten Iversen, HMS-rådgiver
- Leif E. Broch, informasjonssjef
- Wenche Berge Andreassen, arkivleder
- Turid Verstad, IKT-leder
- Ketil Helgevold, rådmann (fra. kl. 10.00)

2.2 Fra Datatilsynet:

- Knut B. Kaspersen, fagdirektør
- Ted Tøraasen, overingeniør

3 Generelt

Eigersund kommune har ca. 15.000 innbyggere, hvorav ca. 1400 er ansatt i kommunen. Det er et visst samarbeid med de andre kommunene i Dalane regionsenter (Bjerkreim, Lund og Sokndal), bl.a. i forhold til PPT og barnevern. Kommunen har en tosone-modell (sikker og åpen sone).

Næringsvirksomheten er sterkt rettet mot oljeindustrien, bl.a. med Aker Solution etablert i kommunen.

4 Oversendelse av dokumentasjon

Datatilsynet ba i varselet av 4. april 2014 om at virksomheten oversendte følgende dokumentasjon:

a) oversikt over virksomhetens organisering, eksempelvis i form av organisasjonskart,
b) styrende dokumenter for internkontroll og informasjonssikkerhet, jf. §§ 13 og 14, og forskriften kapittel 2 og 3,
c) oversikt over personopplysninger som behandles,
d) oversikt over informasjonssystemets utforming, eksempelvis i form av konfigurasjons- eller systemkart,
e) risikovurderinger av informasjonssystemet, jf. forskriften § 2-4,
f) avviksrutiner, jf. forskriften § 2-6,
g) navn og funksjon på de som deltar fra virksomheten under kontrollen, dersom dette er avklart.

I forkant av kontrollen fikk Datatilsynet tilsendt et organisasjonskart, og to nettverkskart.

En detaljert agenda ble oversendt virksomheten før kontrollen.

5 Nærmere om kontrollen

Under kontrollen ble virksomhetens internkontrollsystem og sikkerhetsdokumentasjon gjennomgått på overordnet nivå. Tilsynet hadde fokus på behandlingsansvarliges arbeid med å sørge for etterlevelse av gjeldende lover og forskrifter.

Internkontroll danner en viktig basis i behandlingsansvarliges arbeid med å sørge for etterlevelse av gjeldende lover og forskrifter. Internkontroll er et ledelsesansvar.

6 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

6.1 Internkontroll

6.1.1 Generelt om § 14

Rettslig grunnlag

Virksomheten har etter § 14 plikt til å etablere og holde ved like systematiske tiltak som er nødvendige for å oppfylle kravene i personopplysningslovens regelverk gitt i medhold av denne. Bestemmelsen er utdypet i forskriften kapittel 3.

Internkontrollsystemet omfatter også nødvendig sikkerhetsdokumentasjon. Dette er nærmere omtalt i kapittel 6.2.

Tilsynet ønsket innledningsvis en redegjørelse for hvilke systematiske tiltak virksomheten hadde satt i verk for å sikre etterlevelse av lovens krav. I henhold til § 14 skal behandlingsansvarlig dokumentere tiltakene. Dokumentasjonen skal blant annet være tilgjengelig for medarbeiderne hos den behandlingsansvarlige samt for Datatilsynet.

Internkontrollen omfatter styrende, gjennomførende og kontrollerende dokumenter.

Faktiske forhold og vurdering
Kommunen har ikke etablert noe internkontrollsystem etter § 14. Dette begrunnes med dårlig økonomi og manglende prioritering.

Konklusjon
Det er et avvik etter § 14 at det ikke er etablert noe internkontrollsystem.

6.1.2 Ansvarsforhold etter loven - behandlingsansvarlig

Rettslig grunnlag
Behandlingsansvar defineres i § 2 nr. 4 som: *"den som bestemmer formålet med behandlingen av personopplysninger og hvilke virkemiddel som skal brukes"*. Det er den behandlingsansvarlige som er pliktsubjekt etter personopplysningsloven. Det er derfor av avgjørende betydning for enhver virksomhet hvor behandlingsansvaret er lagt.

Forskriften § 2-3 Sikkerhetsledelse understreker at det er den behandlingsansvarlige som skal sørge for tilfredsstillende informasjonssikkerhet ved at det blant annet opprettes en sikkerhetsorganisering med klare roller, ansvar og myndighet. Dette er nærmere omtalt i kapittel 6.2.

Forskriften § 2-7 understreker at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.

Faktiske forhold
Behandlingsansvaret etter personopplysningloven er ikke tydeliggjort. Heller ikke delegasjonslinjene er tydelige. I den grad det finnes rutiner, er disse ikke dokumenterte.

Konklusjon
Manglende dokumenterte rutiner i tilknytning til behandlingsansvaret er et avvik fra §§ 14 og 13 jf. forskriften § 2-7.

6.1.3 Oversikt over behandlinger og behandlingsgrunnlag

Rettslig grunnlag

For at den behandlingsansvarlige skal ha oversikt over omfanget av sitt ansvar må virksomheten ha en oversikt over hvilke behandlinger av personopplysninger som foretas og hvilke opplysninger som inngår i disse. Dette er en nødvendig del av virksomhetenes internkontroll etter § 14. Oversikten er nødvendig for å sikre at grunnvilkårene i § 11 er oppfylt. Videre danner oversikten grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og sikkerhetsstrategi og vil være underlag ved virksomhetens risikovurderinger. Kravet til oversikt over behandlinger følger derfor også av forskriften § 2-4.

Oversikten over behandlinger må blant annet omfatte behandlingsgrunnlag (§§ 8 og 9) for den enkelte behandling, samt formålet med behandlingen (§ 11). Alternativt må angivelse av behandlingsgrunnlag og formål fremkomme et annet sted i dokumentasjonen. Kravene til oversikt over behandlinger og behandlingsgrunnlag er utdypet i kapittel 3.5 i veilederen *Internkontroll og informasjonssikkerhet* som Datatilsynet refererte til under kontrollen. Her fremkommer blant annet et eksempel på hvordan oversikten kan utformes.

Faktiske forhold og vurdering

Det er ikke utferdiget en oversikt over personopplysninger som behandles i kommunen.

Konklusjon

Manglende oversikt over behandlinger som behandles i kommunen er et avvik fra §§ 14 og 13, jf. forskriften § 2-4.

6.1.4 Øvrige plikter etter § 14 jf. forskriften § 3-1

Behandlingsansvarlige må i henhold til § 14 kartlegge relevante plikter i personopplysningsloven. Aktuelle plikter vil blant annet omfatte plikt til å gi innsyn etter § 18, informasjonsplikt etter §§ 19 og 20, samt vurdering av personopplysningenes kvalitet etter §§ 27 og 28. Oversikten over plikter inngår i den *styrende* delen av internkontrollen. Etter at kartleggingen er gjennomført må det utarbeides rutiner for ivaretakelse av de kartlagte pliktene. Dette er en del av den *gjennomførende* delen av internkontrollen. Slike rutiner kan for eksempel omfatte prosedyrer for innhenting av samtykke og retningslinjer for utlegging av postlister og saksdokumenter på Internett.

6.1.4.1 Rett til innsyn

Rettslig grunnlag

Det følger av § 18, 1. ledd at enhver som ber om det skal få vite hva slags behandling av opplysninger behandlingsansvarlig foretar. Den registrertes rett til innsyn følger også av bestemmelsens andre ledd. Virksomheten skal etter forskriften § 3-1, tredje ledd bokstav d) ha rutiner for å sikre at innsyn foretas i samsvar med bestemmelsene i loven.

Unntak fra retten til innsyn følger av §§ 18 siste ledd og 23.

Faktiske forhold og vurdering:
Kommunen har ikke utferdiget dokumenterte rutiner i forhold til innsynsretten etter § 18, 1. ledd (enhvers krav på innsyn) og innsynsretten som den registrerte har etter § 18, 2. ledd.

Konklusjon
Manglede dokumenterte rutiner for ivaretakelse av § 18, 1. og 2. ledd er et avvik fra krav om internkontroll etter § 14, jf. forskriften § 3-1 bokstav d).

6.1.4.2 Informasjonsplikt når det samles inn opplysninger fra den registrerte selv, eller fra andre enn den registrerte

Rettslig grunnlag
Det følger av § 19, 1.ledd at når det samles inn opplysninger fra den registrerte selv skal den behandlingsansvarlige av eget tiltak først informere den registrerte om

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
b) formålet med behandlingen,
c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
d) det er frivillig å gi fra seg opplysningene, og
e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på en best mulig måte, som for eksempel informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og 28.

Det følger av § 20 at en behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, av eget tiltak skal gi informasjon som nevnt i § 19.

Virksomheten skal etter forskriften § 3-1, tredje ledd bokstav d) ha rutiner for å sikre at informasjonsplikten foretas i samsvar med bestemmelsene i loven.
Unntak fra informasjonsplikten følger av personopplysningsloven § 19 siste ledd, § 20 andre og tredje ledd og § 23.

Faktiske forhold
Kommunen har ikke utferdiget dokumenterte rutiner for ivaretakelse av den registrertes krav på informasjon etter §§ 19 og 20.

Konklusjon
Manglede dokumenterte rutiner for ivaretakelse av §§ 19 og 20 er et avvik fra krav om internkontroll etter § 14, jf. forskriften § 3-1 bokstav d).

6.1.4.3 Retting og sletting

Rettslig grunnlag

I henhold til § 11 bokstav e), jf. §§ 27 og 28, skal personopplysninger slettes når de ikke lenger er nødvendige for formålet med behandlingen. Virksomheten er pliktig å ha rutiner for ivareta personopplysningenes kvalitet, jf. § 28. [1] Se forskriften § 3-1, 3. ledd bokstav c).

Faktiske forhold og vurdering

Virksomheten har ikke utferdiget rutiner for ivaretakelse av personopplysningenes kvalitet i forhold til det definerte formålet med behandling av personopplysningene.

Konklusjon

Manglede rutiner for ivaretakelse av §§ 27 og 28 er et avvik fra krav om internkontroll etter § 14, jf. forskriften § 3-1 bokstav c).

6.1.4.4 Melding/konsesjon

Rettslig grunnlag

I henhold til § 33 kreves det konsesjon for å behandle sensitive personopplysninger. Etter § 33 femte ledd gjelder ikke konsesjonsplikten behandling av personopplysninger i organ for stat eller kommune. Hvis behandlingen av personopplysninger er unntatt konsesjonsplikten etter § 33 gjelder hovedregel i § 31 om meldeplikt. Personopplysningslovens forskrifter kapittel 7 har flere unntak fra konsesjonsplikten og/eller meldeplikten.

Faktiske forhold og vurdering

Kommunen har ikke utferdiget rutiner for oppfyllelse av personopplysningslovens regler om melde- og konsesjonsplikt etter §§ 31 – 33. For tiden er det heller ingen meldinger fra kommunen i meldingsdatabasen. Datatilsynet kontrollerte i denne omgang ikke hvorvidt Eigersund gjør behandlinger av personopplysninger som er meldepliktig etter § 31.

Konklusjon

Manglende rutiner for oppfyllelse av personopplysningslovens regler om melde- og konsesjonsplikt etter §§ 31 – 33, er et avvik fra § 14, jf forskriften § 3-1, 3. ledd bokstav f).

6.2 Krav om informasjonssikkerhet

I henhold til § 13 skal virksomheten gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Tiltakene skal være dokumenterte. Kravene til informasjonssikkerhet er utdypet i forskriften kapittel 2.

---

[1] Personopplysningsloven § 11 bokstav e) krever at den behandlingsansvarlige skal rette eller slette, ufullstendige eller overflødige opplysninger. Bestemmelsen presiserer at disse pliktene ikke bare er rettigheter som tilkommer den registrerte, men selvstendige plikter som påhviler den behandlingsansvarlige uavhengig av om den registrerte krever det. Det vises i den sammenheng også til Ot.prp. nr. 92 (1998-1999) side 114.

For øvrig vises det til Datatilsynets hjemmeside, www.datatilsynet.no og veiledningsmateriale som ble overrakt under kontrollen.

6.2.1 Sikkerhetsledelse

Rettslig grunnlag

I henhold til forskriften § 2-3 skal formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi beskrives i sikkerhetsmål. Valg og prioriteringer skal beskrives i en sikkerhetsstrategi. Bruk av informasjonssystemet skal jevnlig, eksempelvis årlig, gjennomgås for å kartlegge om den er hensiktsmessig for virksomhetens behov og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat. Sikkerhetsstrategier vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet i virksomheten.

Forskriften § 2-7 stiller krav om at det skal etableres klare ansvars- og myndighetsforhold (sikkerhetsorganisasjon).

Sikkerhetsmål og sikkerhetsstrategi

Faktiske forhold og vurdering

Kommunen har ikke fremlagt noen dokumentasjon for sikkerhetsledelse, sikkerhetsmål eller sikkerhetsstrategi. Intervjuet med kommunen ga et ytterligere inntrykk av manglende ledelse av dette området og uklare sikkerhetsmål.

Konklusjon

Manglende sikkerhetsmål og -strategi, er et avvik fra loven § 13, jf. forskriften § 2-3. Avviket understøttes av manglende ledelsesforankring.

Sikkerhetsorganisasjon

Faktiske forhold og vurdering

Kommunen har ikke fremlagt noen dokumentasjon for sikkerhetsorganisasjon. Intervjuet med kommunen ga et ytterligere inntrykk av manglende ledelse og uklare ansvarsforhold. Innkjøp av nye systemer som driftes og administreres av superbrukere (lærere), uten at IT-ansvarlig er med i beslutningsløpet, er et tydelig eksempel. Fragmenteringen og mangelen på oversikt og ansvarsavklaringer gjør det tilnærmet umulig å følge opp og ivareta informasjonssikkerheten.

Konklusjon

Manglende sikkerhetsorganisering er et avvik fra § 13, jf. forskriften § 2-3. Kommunen må sørge for at det finnes klare dokumenterte roller og ansvarsforhold når det gjelder informasjonssikkerhet.

6.2.2 Risikovurdering

Rettslig grunnlag

I henhold til forskriften § 2-4 skal det føres en oversikt over hvilke personopplysninger som behandles. Det skal fastsette kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. På bakgrunn av dette skal den behandlingsansvarlige foreta risikovurderinger for å kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny

risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko. Resultatet av risikovurderingen skal dokumenteres.

Faktiske forhold og vurdering
Kommunen har ikke fremlagt noen dokumentasjon for risikovurdering. Intervjuet med kommunen ga et inntrykk av at systemene under IT-avdelingens kontroll har blitt risikovurdert i en hvis grad, men det er ikke dokumentert.

Det finnes også systemer i kommunen som ikke er underlagt IT-avdelingens kontroll. Disse systemene administreres av superbrukere (lærere). Dette synliggjør manglende kontroll med informasjonssikkerheten.

En overordnet ROS-analyse for beredskap i oktober 2013 var kritisk til mangelen av risikovurderinger for informasjonssikkerhet. Det er derfor ikke tvil om at kommunen var klar over mangelen.

Konklusjon
Manglende risikovurderinger er et avvik fra loven § 13, jf. forskriften § 2-4.

6.2.3 Sikkerhetsrevisjon
Rettslig grunnlag
Virksomheten plikter i henhold til forskriften § 2-5 å gjennomføre sikkerhetsrevisjoner jevnlig, eksempelvis årlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering og at sikkerhetstiltak som er besluttet etablert faktisk er iverksatt og fungerer etter sin hensikt. Resultatet av sikkerhetsrevisjon skal dokumenteres.

Sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerhet i virksomheten. Resultatet fra sikkerhetsrevisjonen vil være en del av grunnlaget for ledelsens gjennomgang jf. forskriften § 2-3.

Faktiske forhold
Kommunen har ikke fremlagt noen dokumentasjon på sikkerhetsrevisjoner.

Konklusjon
At det ikke er gjennomført sikkerhetsrevisjoner er et avvik fra § 13 jf. forskriften § 2-5.

6.2.4 Avvikshåndtering/sikkerhetsbrudd
Rettslig grunnlag
Det følger av forskriften § 2-6 at virksomheten skal ha rutiner for avvikshåndtering. Resultatet fra avviksbehandling skal dokumenteres. Etter forskriften § 2-8, 2. ledd skal medarbeidere ha nødvendig kunnskap for å bruke informasjonssystemet i tråd med de rutiner som er fastlagt. Det er således et krav til at de foreliggende rutiner må implementeres i virksomheten.

For de tilfeller der avvik har avdekket uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet orienteres.

Faktiske forhold og vurdering
Kommunen informerte om at de hadde rutiner for avvik. Dette inkluderte også avvik innen for informasjonssikkerhet. Det var rapportert så få avvik at kommunen så for seg at kunnskapen om avvikssystemet var mangelfull hos de ansatte. Hvis avvikssystemet skal fungere etter hensikten må opplæringen bli bedre.

Konkrete rutiner for avvik ble ikke gjennomgått under kontrollen.

Konklusjon
Kommunes redegjørelse er lagt til grunn, og det ble ikke konstatert avvik.

Det bemerkes at det bør tas inn i avviksrutinen om avviket skal meldes til Datatilsynet i henhold til forskriften § 2-6.

6.2.5 Sikkerhetstiltak

Rettslig grunnlag
Forskriften §§ 2-11, 2-12 og 2-13 stiller om at det gjennomføres tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet.

Forskriften § 2-14 pålegger at det skal innføres sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Videre pålegger forskriften § 2-8, 3. ledd og § 2-14 annet ledd at henholdsvis autorisert og uautorisert bruk av informasjonssystemet skal registreres.

Faktiske forhold og vurdering
Kommunen har en tosone-modell med saksbehandling i sikker sone. Tilganger og rettigheter til fagsystemer styres av superbrukere, og IT-avdelingen har ikke tilgang. Hjemmekontor kjøres via VPN-tunell med to-faktor autentisering og terminal server. Det er rutiner for hvem som har fysisk tilgang til serverrom. Sikkerhetskopiering blir gjort rutinemessig og lagres på en annen fysisk lokasjon. Det er mulig å hente ut informasjon fra sikker sone til minnepinner.

Epost-systemet er delt i to, en del er under kontroll av IT-avdelingen og den andre administreres av superbrukere. Dette er skolene som har sitt eget epost system. Informasjonen rundt dette var uklar, men man lurte på om dette var en del av opplæringsplattformen Moava.

Konklusjon
At brukere kan overføre data ved hjelp av minnepinner ut av sikker sone, uten at det er etablert kompenserende sikkerhetstiltak, gir ikke tilfredsstillende konfidensialitetssikring. Som det fremgår tidligere i rapportens punkt om risikovurderinger, er ikke dette vurdert tilstrekkelig av kommunen selv.

Kommunen kan ikke gi klart svar på hvordan eposten administreres og hvilke sikkerhetstiltak som ligger til grunn for lærernes epost.

Manglende begrensning i bruk av bruk av minnepinner gir er at avvik fra krav om konfidensialitetssikring etter § 13, jf. forskriften §§ 2-11 og § 2-14.

Manglende dokumentasjon av sikkerhetstiltak er at avvik fra § 13, jf. forskriften § 2-14.

6.2.6 Opplæring

Rettslig grunnlag

I henhold til forskriften § 2-8 skal medarbeideren ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med fastlagte rutiner. Dette medfører at de rutiner som utformes med bakgrunn i de øvrige bestemmelser må implementeres i virksomheten, og at de ansatte må gis den opplæring som er nødvendig for å kunne følge dem.

Faktiske forhold og vurdering

Kommunen har ikke dokumenterte rutiner for opplæring av alle nyansatte.

Konklusjon

Manglende rutiner for opplæring av ansatte er et avvik i fra § 13, jf. forskriften § 2-8.

6.3 Databehandlere

Rettslig grunnlag

En *databehandler* er i § 2 nr. 5 definert som *den som behandler personopplysninger på vegne av den behandlingsansvarlige.* Dersom andre virksomheter behandler personopplysninger på vegne av kommunen må det inngås en skriftlig databehandleravtale med virksomheten, jf. § 15. I avtalen skal det fremgå at databehandleren plikter å gjennomføre tiltak for å ivareta tilfredsstillende informasjonssikkerhet, jf. § 13.

Databehandler har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet, jf. § 13. Databehandler kan bare behandle opplysninger slik som det er avtalt med den behandlingsansvarlige.

Faktiske forhold og vurdering

Kommunen mangler rutiner for opprettelse av nye databehandleravtaler. Det finnes ingen oversikt over eventuelle eksisterende avtaler. Kommunen funger som databehandler for andre uten at avtaleforholdene er regulert av databehandleravtaler.

Konklusjon

Manglende oversikt over databehandlere og kontroll med om det er inngått avtaler med disse er et avvik etter § 14 jf. forskriften § 2-15 og § 15.