Reglement - informasjonssikkerhet og personvern

Formål

Formålet med reglementet er å sikre tilstrekkelig styring og kontroll (internkontroll) innen informasjonssikkerhets- og personvernområdet. Reglementet skal ligge til grunn for utøving av styring og kontroll slik at opplysningene blir behandlet lovlig, sikkert og forsvarlig.

Formålet med informasjonsbehandling i kommunen er å understøtte kommunens oppgaver og tjenester slik at vi kan nå våre mål og realisere vår visjon. En informasjonsbehandling som er målorientert, effektiv, lovlig og til å stole på er avgjørende for at kommunen skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette.

Omfang/Virkeområde

Karmøy kommune er behandlingsansvarlig og har ansvar for å etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av overnevnte lover.

Ansvar og myndighet for informasjonssikkerhet og personvern skal følge det ordinære linjeansvaret. Ledere (virksomhetsledere) som har ansvar for mål, arbeidsoppgaver og tjenester skal også ha ansvaret for tilhørende informasjonsbehandling (herunder også behandling av personopplysninger), IKT-system og informasjonssikkerhet.

Ansvar

Informasjonssikkerhet

Arbeidet med informasjonssikkerhet baseres på Difis veileder «Internkontroll i praksis – informasjonssikkerhet» og Normen (Norm for informasjonssikkerhet, helse og omsorgstjenesten).

Personvern

Alle ledere som innen sitt ansvarsområde behandler personopplysninger har ansvar for implementering av denne prosedyren - og for at prosedyren til enhver tid etterleves.

Aktivitet/beskrivelse

Strategi og mål

Informasjonssikkerhets- og personvernstrategien skal ligge til grunn for all behandling av informasjon og personopplysninger i kommunen. Arbeidet skal følges opp gjennom kommunens forbedringssystem.

Gjennom forankring, forpliktelse og forståelse vil Karmøy kommune oppnå effektiv sikkerhetsstyring. Kommunen har følgende prioriteringer for å oppnå dette:

- Videreutvikling av forbedringssystemet Compilo
- Tydelig ledelsesforankring og styrking av sikkerhetskulturen (bevisstgjøring)

Videreutvikling av forbedringssystemet Compilo

Forbedringssystemet vil bestå av ulike steg som skal sikre en kontinuerlig prosess for å bedre informasjonssikkerheten og personvernet i kommunen.

Tydelig ledelsesforankring og styrking av forbedringskulturen

Forbedringsarbeidet må forankres i ledelsen, baseres på en tydelig ansvarsfordeling, og med et kontinuerlig fokus på bevisstgjøring, motivasjon og kompetanseheving.

Den viktigste bidragsyter i forbedringsarbeidet er imidlertid den enkelte ansatt. Men arbeidet må forankres i hele linjen, hvor summen av kunnskap, motivasjon, holdninger og adferd bidrar til styrking av kommunens sikkerhetskultur.

Mål

Vår behandling av informasjon er i samsvar med lover, regler og avtaler, og bidrar på en formåls- og kostnadseffektiv måte til best mulig realisering av kommunens målkart.

Tilgjengelighet:

Personopplysninger og IKT-løsninger er tilgjengelige for ansatte med tjenestlige behov, innbyggere om egne opplysninger og næringsliv om næringsrettede opplysninger.

Kvalitet/integritet:

Informasjon blir bare produsert og endret av de som har fullmakt til det. Informasjon blir ikke endret utilsiktet og skal til enhver tid være relevant og korrekt.

Konfidensialitet:

Kun personer/ansatte med rett til informasjonen får tilgang til den.

Internkontroll – styring og kontroll av personvernet

Etablering av internkontroll er en sentral del av kommunens helhetlige strategi for behandling av personopplysninger. Hvordan kommunen håndterer opplysninger om ansatte, innbyggere, brukere, elever eller andre, er sentralt for å oppnå tillit både innad hos egne ansatte og utad hos våre tjenestemottakere. Det vil kunne påvirke kommunens omdømme hvis den generelle oppfatningen er at kommunen ikke respekterer de ansattes eller innbyggernes rettigheter.

Internkontroll reduserer risikoen for hendelser som krenker personvernet til de kommunen behandler personopplysninger om. Enkeltstående hendelser som representerer brudd på personvernregelverket, eksempelvis uautorisert utlevering av personopplysninger eller brudd på meldeplikten, vil kunne utløse overtredelsesgebyr og føre til negativ omtale og omdømmetap.

Behandling av personopplysninger

Karmøy kommune skal ha en oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke opplysninger som inngår i disse (GDPR art. 30). Oversikten skal føres i henhold til *prosedyre for utarbeidelse av oversikt over behandlinger*.

Oversikten er nødvendig for at organisasjonen skal kunne ivareta pliktene sine. Oversikten skal brukes som underlag ved risikovurderinger.

Begrunnelse for behandling av personopplysninger

Det er ikke tillatt å behandle personopplysninger uten at det er definert et formål med behandlingen. Personopplysningsloven § 8 og Artikkel 5 og 9 i GDPR gir vilkår for å behandle personopplysninger. Kort oppsummert kreves det at

- Den registrerte har gitt samtykke til behandlingen
- Behandlingen er nødvendig for å oppfylle en avtale
- Behandlingen er hjemlet i lov

Se videre *prosedyre for behandling av personopplysninger* for mer informasjon.

Behandling av personopplysninger medfører plikter. Ulike opplysninger og ulike formål medfører at ingen virksomhet er like. Hver etat/virksomhet må derfor identifisere plikter og tilpasse internkontroll og informasjonssikkerhetstiltak til sin organisasjon.

Personvernerklæring

GDPR stiller konkrete krav i Artikkel 13 til at kommunen må utarbeide personvernerklæringer vedrørende hvordan kommunen samler inn og bruker personopplysninger. Kommunen skal ved innsamling av personopplysninger gi nødvendig informasjon for å sikre en rettferdig og gjennomsiktig behandling.

Risikovurdering

Ved innføring av internkontroll, må organisasjonen først identifisere hvilke personopplysninger som behandles. Deretter må det utarbeides en risikoanalyse med vurderinger av risiko for at en uønsket hendelse skjer, både innen personopplysninger og informasjonssikkerhet, og eventuelle konsekvenser av dette. Risikovurderingen danner grunnlag for iverksettelse av nødvendige sikkerhetstiltak og inngår i underlag for ledelsens gjennomgang av styringssystemet.

Se *prosedyre for risikohåndtering* for mer informasjon.

Akseptabelt risikonivå

For å kunne fastsette hva akseptabelt risikonivå er, skal behov for konfidensialitet, tilgjengelighet og integritet vurderes. I noen situasjoner kan disse tre komme i konflikt med hverandre. Særlig vil behov for konfidensialitet og tilgjengelighet kunne være vanskelig å forene. Det er viktig at kryssende hensyn identifiseres, og at prioritering

mellom forskjellige behov fremgår i beskrivelsen av akseptabelt risikonivå.

Dokumentasjon

Gjennomførte vurderinger og tiltak skal dokumenteres. Dokumentasjonen skal være tilgjengelig for medarbeiderne og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernombudet.

Oversikt over elektroniske systemer

Oversikt over elektroniske systemer som behandler data er tilgjengelig i Arkivplanen;

http://karmoy.arkivplan.no/content/view/full/10201

Kontinuerlig forbedring – ledelsens gjennomgang

Etter at internkontrollen er etablert og forankret, må det sørges for at den gjøres kjent og etterleves blant de ansatte.

Ledelsen skal årlig gjennomgå mål, strategi og organisering av styringssystemet. Ledelsen skal kontrollere at disse er i samsvar med kommunens behov og eventuelt oppdatere dem. Gjennomgangen utføres i henhold til *prosedyre for ledelsens gjennomgåelse*.

Avvikshåndtering

Ved brudd på personopplysningssikkerheten skal det innen 72 timer etter å ha fått kjennskap til avviket, melde bruddet til Datatilsynet gjennom skjema i Altinn (GDPR Art. 33). Det er kun ved hendelser hvor det er *lite trolig* at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter at Datatilsynet ikke skal varsles. Ved usikkerhet rundt varslingsplikten til Datatilsynet, vil personvernombudet kunne hjelpe.

Hendelser som kan påvirke målene for informasjonssikkerhet negativt, skal meldes og følges opp på en systematisk måte. Videre *skal prosedyre for melding og håndtering av avvik* følges for intern melding og håndtering av hendelsen.

Kompetanse

Før ansatte i organisasjonen og eventuelle tredjepartsbrukere får tilgang til IKT-systemer skal de få hensiktsmessig opplæring. Dette omfatter krav til internkontroll og informasjonssikkerhet, juridisk ansvar og interne sikringstiltak, så vel som opplæring i riktig bruk av informasjonssystemer.

Krav til ansatte

Alle ansatte skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon og personopplysninger de behandler og hvilke krav som stilles til behandlingen og bruken av IKT.

Alle ansatte skal etterleve de lover, regler, retningslinjer, krav, prosedyrer, instrukser mv. som gjelder for dem og det arbeid de utfører.

Hjemmel

Personopplysningsloven

Forskrift:
eForvaltningsforskriften

Referanser

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) stiller krav til at forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for organisasjonens styring og kontroll på informasjonssikkerhetsområdet.

GDPR (General Data Protection Regulation)setter krav vedrørende regler for vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler for fri utveksling av personopplysninger. Videre kreves vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak for å oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet.