

Policy for informasjonssikkerheit og personvern

Dette er Ålesund kommune sin hovedstrategi for informasjonssikkerheit og personvern, der målet er å sikre og beskytte informasjonen i kommunen.

Mål

Målet er å sikre at ein er innanfor kommunen sin grense for akseptabelt risikonivå gjennom god risikostyring, og å unngå at behandling av personopplysningar medfører høg risiko for dei registrerte sine rettar etter personvernforordninga. Databehandling (elektronisk og anna) i forbindelse med utøving av kommunale oppgåver og tenester skal foregå på ein sikker måte, både eksternt og internt. Test av kommunen sitt datautstyr, datasystem og informasjonsflyt skal oppfylle offentlege krav til konfidensialitet, integritet og tilgjengelighet

For å oppnå dette legg vi vekt på å vere opne, bygge god kompetanse internt og sikre kontroll med våre leverandørar.

Derfor er det viktig at datasystem og nettverk er designa og vert drifta på ein slik måte at data alltid kan nåast, men det er og viktig at det finns manuelle rutiner som kan overta dersom datasystem likevel av ein eller annan grunn skulle vere utilgjengeleg for ein periode.

Omfang

Strategien for personvern og informasjonssikkerheit gjeld all informasjonsbehandling som skjer internt i kommunen og som kommunen har ansvaret for eksternt. Dette omfattar all behandling, lagring og kommunikasjon av informasjon både munnleg, på papir og digitalt. All bruk av IKT-verktøy er og inkludert. Strategien gjeld alle tilsette i Ålesund kommune.

Ivaretaking av personvernet til innbyggjarar og tilsette

Ålesund kommune forvaltar personopplysningar om alle tilsette og alle innbyggjarane i kommunen. Disse opplysningane skal vi behandle med respekt for den enkelte registrerte og i samsvar med krav som fylgjer av regelverket. At dette blir ivareteke er naudsynt for bruken av opplysningane i ein digitalisert kvardag, og for å ivareta tillita frå dei registrerte.

Grunnleggande er det at kommunen følger personvernprinsippa slik dei er definert i GDPR artikkel 5:

"Lovlighet, rettferdighet og gjennomsiktighet

Formålsbegrensning

Dataminimering

Riktighet

Lagringsbegrensning

Integritet og fortrolighet

Ansvar"

Sikring av informasjonsverdiar

Vår handsaming av informasjon skal til ein kvar tid vere i samsvar med lover, reglar og avtalar.

Kommunen skal ha god sikring av informasjonsverdiane i IKT systema våre og ei tilgjengelegheit i IKT-løysingane som er naudsynt for å levere kommunale tenester.

Vi erkjenner at informasjonen vi forvaltar har ein vesentleg verdi, og at vi er eit potensielt mål for eksterne aktørar som har interesse i å tileigne seg informasjon, endre informasjon, slette informasjon, gjere våre tenester utilgjengelege eller oppnå kontroll eller skade på vår fysiske infrastruktur.

Dette føreset god styring av informasjonssikkerheitsarbeidet, god kultur og gode tekniske løysingar.

Vi skal ivareta dei tilsette sitt personvern i utforminga av IKT-løysningar og IKT-sikringstiltak. Arbeidet må skje i samspel med dei tillitsvalte. Ved inngripande sikringsløysingar skal det gjerast vurderingar av personvernkonsekvensane før tiltaket iverksettast.

Våre informasjonsverdiar skal gjennom system og rutiner sikrast etter prinsippa om tilgjengelegheit, integritet og konfidensialitet, og våre system skal vere robuste:

- *Tilgjengelegheit* er at informasjonen er tilgjengeleg for autoriserte brukarar når det er behov for data.
- *Integritet* er at informasjonen som blir lagra alltid skal vere korrekt og fullstendig. Det er defor viktig at ingen andre enn dei som er autorisert har høve til å endre eller slette data
- *Konfidensialitet* er at informasjon berre kan lesast av dei som er autoriserte og har behov for informasjonen i sitt arbeid. Brot på teieplikta vil vere eit brot på konfidensialiteten.

Organisering

Roller

- **Kommunedirektør** har det overordna ansvar for å ivareta personvern og informasjonssikkerheit.
 - Kommunedirektør svarer ut behandlingsansvarlig sine plikter i administrasjonen.
 - Kommunedirektør sine oppgåver kan ivaretakast i leiargruppa.
- **Behandlingsansvarleg** er den (fysisk eller juridisk person, offentleg mynde) som bestemmer formålet med behandling av personopplysningar og kva hjelpemidlar som skal brukast. Behandlingsansvarleg er identisk med begrepet **Dataansvarleg** som helselovgjevinga og Normen (Direktoratet for e-helse) nyttar.

Den behandlingsansvarlege er det primære pliktsubjektet etter GDPR-forordninga, og er overordna ansvarleg for å overhalde personvernprinsippa og regelverket. Det vil sei å behandle personopplysningar på ein lovleg, rettferdig og gjennomsiiktig måte, og sikre at det føreligg eit behandlingsgrunnlag. Behandlingsansvarleg har ansvaret for at det er etablert alle naudsynte organisatoriske og tekniske tiltak for å sikre at ein overheld regelverket.

- Ansvar og mynde for informasjonssikkerheit skal følge det ordinære linjeansvaret.
- Kommunen skal ha eit **personvernombod** som har som oppgave å føre kontroll med og gje råd om korleis kommunen best mogleg kan ivareta personverninteressene. Personvernombudet skal konsulterast aktivt i personvernarbeidet. Kommunen har engasjert IKA M&R i rolla som personvernombud.
- **Informasjonssikkerheitsansvarleg** har utøvande ansvar for å kontrollere og koordinere det førebyggjande personvern- og sikringsarbeid. Informasjonssikkerheitsansvarleg er underlagt stabssjef for det som gjeld den daglege drifta. Ved regelmessig rapportering og i særskilte tilfelle rapporterer informasjonssikkerheitsansvarleg direkte til kommunedirektør.

Informasjonssikkerhetsansvarleg:

- utarbeider tiltak for kulturbygging og internkontroll i heile organisasjonen.
 - har ansvar for å avdekke risikoar og gjere naudsynte tiltak.
 - skal vedlikehalde ei oversikt over behandlingar av personopplysingar i samsvar med regelverket.
 - skal vedlikehalde ei oversikt over våre informasjonsverdiar/komponentar.
- **Systemeigar** er eigar av fagsystema som naturleg høyrer inn under området ein leier, og skal sørge for at systema er hensiktsmessige og oppdatert, nødvendige rutiner etablert, og at naudsynte vurderingar av personvernkonsekvensar og risikovurderingar er gjennomførte. Systemeigar skal ivareta interessene til dei som nyttar systema i si oppgåveløysing, og involvere desse på hensiktsmessig måte i systemforvaltning. Systemeigarskap skal identifiserast med tittel, og skal gis ein leiar. Systemeigar kan i instruks delegere oppgåver til ein **systemansvarleg**. Systemeigar kan oppnemne systemansvarleg som skal ha operativt ansvar for dei oppgåver systemeigar har ansvar for. Systemeigar kan og gje systemansvarlege hovedansvar for å gje opplæring til brukarar, samt utføre risikoanalyse.
 - **IKT-driftsansvarleg** (avdelingsleiar IKT-drift), skal implementere overordna føringar i sitt sikringsarbeid på det tekniske nivået.
 - Oppgåver for informasjonssikkerheitsansvarleg, systemeigar og systemansvarleg skal inngå i styringssystemet for informasjonssikkerheit.

Styring

Styring av personvern- og informasjonssikkerheitsarbeidet skal vere ein integrert del av internkontrollarbeidet i kommunen.

Toppleiinga skal minimum halvårleg ha gjennomgang av arbeidet med personvern og informasjonssikkerheit. Som ein del av dette skal trussel- og risikobilete, hendingar sidan sist og status i påbyrja prosessar gjennomgåast

Strategi for informasjonssikkerhet

Krav til internkontroll- og sikkerhetsarbeidet

- Vi skal følge anerkjente prinsipper for styring av informasjonssikkerhet
- Vi må ha en tydelig sikkerhetsorganisasjon, med klare ansvarsområder
- Arbeidet med informasjonssikkerhet skal være forankra i ein internkontroll (styring og kontroll) basert på anerkjente standarder på informasjonssikkerhetsområdet
- Vi må ha tilstrekkelig kompetanse på informasjonssikkerhet i alle ledd
- Alle tilsette skal involverast i arbeidet med informasjonssikkerhet, minimum gjennom e-læring og at forhold kring informasjonssikkerhet blir drøfta på arbeidsplassen regelmessig.
- Arbeidet skal følge gjeldande lover, reglar og avtalar
- Vi må ha eit oppdatert, godt kommunisert og lett tilgjengeleg regelverk
- Vi må vere proaktive i forhold til trusselbilde, og ligge i forkant med tiltak
- Vi må ha beredskapsplanar for å handtere bortfall av datatenester
- Vi skal systematisk vurdere behov for - og gjennomføre nødvendige risikovurderingar
- Våre underleverandørar av IKT-løysingar og databehandlarar skal reviderast regelmessig, enten ved tredjepartsrevisjonar eller ved at vi gjennomfører revisjonar.
- Risikoreduserande tiltak skal vere basert på risikovurderingar, DPIA, vesentligheit, nytte-kost vurderingar og leiinga sine føringar for risikohandtering og eit effektivt sikkerhetsarbeid
- Hendingar som kan påverke måla for informasjonssikkerhet negativt, skal meldast og følgast opp på ein systematisk måte
- Leiarar på alle nivå skal systematisk styre, kontrollere og følge opp tilstand og arbeid med informasjonssikkerhet i eiga eining
- Arbeidet med informasjonssikkerhet skal evaluerast systematisk
- Alle avvik skal meldast, også sjølv om dei ikkje har hatt negativ konsekvens.
- Regelverk og tekniske løysingar må støtte opp under IT-strategi og virksomhetsarkitektur
- Vi skal følge beste praksis for sikringstiltak, og vi skal regelmessig gjennomføre penetrasjonstestar og sårbarhetsskanning
- Kommunen skal vere tilknytt ein varslingsinfrastruktur for IKT-truslar og hendingar (CERT), og vi skal respondere adekvat på varsel som kjem inn, og sjølv varsle når det er relevant. Det skal vere etablerte rutiner for varsling og hendelseshandtering, til dømes ved behov for å stenge tenester.

Krav til leverandører

- Vi skal sikre at løysingane våre er utvikla i samsvar med prinsippa for innebygd personvern. Dette må vi gjere ved å sette krav om det til leverandørane og følge dei opp.
- Databehandlaravtale skal inngås med alle eksterne som lagrar og behandlar våre data
- Gjennom databehandlaravtale skal vi sikre at personopplysningar berre vert behandla innanfor EU/EØS (med mindre anna vert avtala skriftleg) og ikkje i land som skårar under 70 på Transparency International corruption perception Index. Dersom avtalen gjeld behandling av sensitive personopplysningar skal behandling av slike opplysningar skje i Norge. Behandlingsansvarleg kan tillate at behandling av sensitive personopplysningar skjer utanfor Norge. Slik behandling krev skiftleg førehandsgodkjenning, og samtykke kan nektast på fritt grunnlag.
- Ved mogeleg brot på personvern eller informasjonssikkerhet, skal leverandør skriftleg varsle kommunen utan ugrunna opphald

Krav til tilsette

- Alle tilsette skal ha eit bevisst forhold til måla for eige arbeid, kva informasjon dei behandlar og kva krav som vert stilt til informasjonsbehandling og bruk av IKT
- Alle tilsette skal etterleve dei lover, reglar, retningsliner, krav, prosedyrer, rutiner mv. som gjeld for dei og det arbeid dei utfører

Relevant regelverk

Personopplysningslova (med personvernforordninga), helseregisterlova, pasientjournallova, helseforskningslova, forvaltningslova (§15a), eForvaltningsforskrift, sivilforsvarslova

Godkjent

Policyen er godkjent i leiargruppa 08.06.2020