Hefte 2

Informasjonssikkerhet

Styrende dokument

Melhus er en mangfoldig kommune
der det skal være mulig å være modig

Godt personvern - din rettighet, vår plikt

Godt personvern sikrer at behandling av personopplysninger skjer innenfor fastsatte krav om:

- *Tilgjengelighet*
- *Integritet*
- *Konfidensialitet*
- *Robusthet*

Grunnleggende personvernprinsipper

Reglene for behandling av personopplysninger bygger på noen grunnleggende prinsipper. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene:

- *Lovlig, rettferdig og gjennomsiktig*
- *Formålsbegrensning*
- *Dataminimering*
- *Riktighet*
- *Lagringsbegrensning*
- *Integritet og konfidensialitet*
- *Ansvarlighet*

De registrertes rettigheter

Alle virksomheter har plikt til å legge til rette for at brukere/kunder får oppfylt rettighetene sine på en enkel måte. Det skal som hovedregel gjøres uten kostnad for kunden og innen 30 dager:

- *Rett til innsyn*
- *Rett til retting*
- *Rett til sletting*
- *Rett til begrensning*
- *Rett til å protestere*
- *Rettigheter ved automatiske avgjørelser*
- *Rett til dataportabilitet*
- *Rett til informasjon*

Innhold

Revisjonsliste

Dato	Versjon	Skrevet av	Endring i forhold til forrige versjon
4.9.2013	2.0	Rodo	Ny utgave, sikkerhetshåndboken delt 2
5.11.2013	2.0	Rodo	Godkjent av rådmannen
9.3..2013	2.1	Rodo	Revidert utgave
16.5.2014	2.1	Rodo	Gjennomgått i ledermøte

1.0 Styrende dokumentasjon

1.1 Innledning

Formålet med styringssystemet for informasjonssikkerhet er å sikre at all behandling av personopplysninger og annen informasjon i Melhus kommune samt bruk av IT-hjelpemidler, skjer innenfor fastsatte krav. Dette er krav til konfidensialitet, integritet, tilgjengelighet, og robusthet. Krav i henhold til lover og forskrifter, samt inngåtte avtaler og interne krav i Melhus kommune.

Styringssystemet for informasjonssikkerhet er utformet med basis i de veiledninger som Datatilsynet har publisert på www.datatilsynet.no, særlig veiledningene om internkontroll som ble publisert november 2009. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Personvernforordningen stiller krav til den behandlingsansvarliges ansvar. Det innebærer å sette i verk egnede tiltak, både tekniske og organisatoriske, for å sikre og påvise at personopplysninger behandles i samsvar med regelverket (internkontroll). Internkontrollen dokumenteres gjennom sikkerhetshåndboken(styrende dokument).

EUs personvernforordning (GDPR) **om vern av fysiske personer i forbindelse med behandling av personopplysninger** er en del av personopplysningsloven.

Personvernforordningen inneholder både rettigheter og plikter knyttet til behandling av personopplysninger. Felles for alle reglene er at de bygger på noen grunnleggende prinsipper for personopplysningsvern (personvernprinsippene) som er beskrevet i forordningen.

Prinsippene gir på ulike måter uttrykk for at behandling av personopplysninger skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltmennesket, se pkt 3.1, datansavarliges ansvar.

1.2 Om sikkerhetshåndboken

Sikkerhetshåndboken utgjør 3 hefter som basis for Melhus kommunes styringssystem for informasjonssikkerhet. Systemet bygger på et felles grunnlag for informasjonssikkerhet med særlig vekt på behandling av personopplysninger i henhold til lover, forskrifter og retningslinjer.

Styringssystemet bidrar til å sikre et felles nivå på informasjonssikkerhet på tvers av virksomhetene i kommunen, og gir felles føringer for kommunens ansatte, eksterne brukere, borgere og samarbeidspartnere.

Sikkerhetshåndboken er delt inn i 3 hefter:

- **Ansatte og sikkerhetskultur** (for alle ansatte)
- **Policy, regelverk, rutiner og prosedyrer** (for ledere)
- **IT-løsning – drift** (for IKT-ansatte og sikkerhetsansvarlig)

Målgruppen for dette dokumentet er ledere og ansatte i IT- og digital samhandling.

For definisjoner se **vedlegg 1**

2.0 Om informasjonssikkerhet

2.1 Grunnleggende personvernprinsipper

Reglene for behandling av personopplysninger bygger på noen grunnleggende prinsipper. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene.

Lovlig, rettferdig og gjennomsiktig
Behandling av personopplysninger må være **lovlig**. Det må finnes et rettslig grunnlag for den behandlingen en virksomhet ønsker å gjøre.
Behandling av personopplysninger må skje **rettferdig.** Behandlingen av personopplysninger skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal dessuten være gjennomsiktig og forståelig for de registrerte, den skal ikke foregå på fordekte eller manipulerende måter.
Behandling av personopplysninger skal være **gjennomsiktig.** Behandling av personopplysninger skal være oversiktlig og forutsigbar for den registrerte. Den det behandles opplysninger om skal være informert om dette.

Formålsbegrensning
Personopplysninger skal kun behandles for **spesifikke, uttrykkelige, angitte og legitime** formål. Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at **alle berørte har samme entydige forståelse** av hva personopplysningene skal brukes til. At formålet skal være **legitimt** innebærer at det i tillegg til å ha et rettslig grunnlag også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer.
Personopplysninger kan ikke gjenbrukes til formål som er uforenlig med det opprinnelige. Hvis personopplysninger skal gjenbrukes må behandlingen enten være lovfestet eller det må innhentes nytt samtykke.

Datminimering
Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet.

Riktighet
Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig. Dette betyr at behandlingsansvarlig må sørge for å straks slette eller rette personopplysninger som er uriktige med hensyn til de formål de behandles for.

Lagringsbegrensning
Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for. Melhus kommune er i det alt vesentligste regulert av arkivloven og …… Dette innebærer at spørsmålet om lagringsbegrensning stort sett vil gjelde tjenester som ikke er lovpålagt f.eks. billettsalg.

Integritet og konfidensialitet
Personopplysninger skal behandles slik at opplysningenes integritet og konfidensialitet beskyttes.

Ansvarlighet
Prinsippet om ansvarlighet understreker den **behandlingsansvarliges** ansvar for å opptre i samsvar med reglene for behandling av personopplysninger.
Det er ikke nok å bare ha ansvaret – man må vise at man tar ansvaret. Den behandlingsansvarlige må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid. Virksomheten må også kunne vise at den faktisk opptrer i samsvar med reglene.

2.2 Mål med IKT i Melhus kommune

- Vi skal sette brukernes behov i sentrum når vi skal vurdere digitale løsninger
- Vi skal utvikle tjenester, og øke produktiviteten i våre tjenester gjennom bruk av digitale verktøy
- Vi skal sikre at alle brukere av digitale verktøy klarer å benytte seg av disse
- Vi skal sikre at digitaliseringsprosjekter gjennomføres på en effektiv måte
- Vi skal sørge for å ha sikre IT-systemer, og behandle personopplysninger på en forsvarlig måte

2.3 Hvorfor informasjonssikkerhet i Melhus kommune?

Innbyggere, brukere, ansatte, politikere og samarbeidspartnere har krav på at Melhus kommune behandler informasjon, herunder personopplysninger, i tråd med de krav som stilles i norsk lov og regelverk.

En viktig del av dette er det personvernforordningen art. 32 kaller personopplysningssikkerhet. Det er det samme som informasjonssikkerhet for personopplysninger.

Informasjonssikkerhet handler om å håndtere risiko relatert til informasjon og behandling av personopplysninger. Informasjonens integritet, tilgjengelighet og konfidensialitet skal sikres. God informasjonssikkerhet er viktig for å kunne utøve forsvarlige tjenester.

Med «integritet» menes at personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting.

Med «tilgjengelighet» menes at helse- og personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Med «konfidensialitet» menes at personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene. Konfidensialitet bidrar til ivaretakelse av taushetsplikt og personvern.

Personvernforordningen bruker også begrepet robusthet i tillegg til integritet, tilgjengelighet og konfidensialitet. Med «robusthet» menes organisasjonens og informasjonssystemenes evne til å gjenopprette normaltilstand etter for eksempel en fysisk eller teknisk hendelse.

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Personopplysninger skal behandles i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene. Personvern er derfor nær knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse.

Personopplysninger skal behandles etter prinsippene i personvernforordningen art. 5, (personvernprinsippene se pkt 3.1) og de registrertes rettigheter skal sikres.

Krav til informasjonssikkerhet er også nedfelt i andre lover, f eks forskrift om ledelse og kvalitetsforbedring i helsetjenesten, offenteglov, sosialtjenestelov, barnevernslov etc., se **vedlegg 2**

.

Alle har rett til å vite hvilke opplysninger Melhus kommune bruker om dem. En forutsetning for at de kan benytte seg av innsynsretten er at kommunen forteller hva de bruker opplysningene til. Alle behandlinger kommer tydelig frem i **Personvernerklæring**, se **vedlegg 3**. Denne erklæringen er gjort tilgjengelig på kommunens nettsted.

2.4 Spesielt om personopplysninger

2.4.1 Tilgjengelighet

Hovedmål:
Personopplysninger skal være tilgjengelig og anvendelig for autorisert personell slik at oppgaver kan utføres til planlagt tid.

Delmål
Kritiske systemer for behandling og lagring av personopplysninger skal som hovedregel være kontinuerlig tilgjengelig for sluttbruker.
Strategi
IKT- løsninger som behandler personopplysninger, skal som hovedregel være dupliserte. Ved avvik fra hovedregel skal risikovurderinger legges til grunn.
IKT-systemene skal være dimensjonert for å ivareta kontinuerlig tilgjengelighet til kritiske systemer målt hos sluttbruker.
Det skal etableres beredskapstiltak for kritiske systemer.
Det skal etableres prosedyrer for sikkerhetskopiering og tilbakelegging av all elektronisk lagret informasjon og konfigurasjoner og sikker oppbevaring av disse.

2.4.2 Integritet

Hovedmål
Alle personopplysninger i kommunen skal til enhver tid være relevante, korrekte, oppdaterte og et resultat av autoriserte og kontrollerte aktiviteter.
Delmål
Det skal være samsvar mellom informasjonen ved informasjonskilden og gjengivelsen av denne informasjonen i systemer som behandler personopplysninger.
Alle registreringer, endringer og slettinger i systemer som behandler personopplysninger skal være et resultat av autoriserte og kontrollerte handlinger.
Alle registreringer og endringer i systemer som behandler personopplysninger skal kunne spores til opprinnelse.
Strategi
Registre med personopplysninger skal lagres på sentrale servere
Det skal etableres prosedyrer for

- behandling av avvik
- logging og oppfølging av logger

Endringer ved systemer som behandler personopplysninger skal kunne følges tilbake til rett bruker.

Historikk skal alltid bevares ved endring av informasjon i systemer som behandler personopplysninger.
Sletting av informasjon i systemer som behandler personopplysninger skal skje i tråd med gjeldende lover og forskrifter.

2.4.3 Konfidensialitet

Hovedmål:
Personopplysninger skal ikke være tilgjengelig for eller bli kjent for uautorisert personell eller uvedkommende internt eller eksternt. Ved konflikt mellom konfidensialitet og tilgjengelighet skal konfidensialitet prioriteres når de to sikkerhetselementene vurderes som like viktige[1].
Delmål:
Personopplysninger skal kun være tilgjengelig for autorisert personell.
Utlevering eller overføring av sensitive personopplysninger som kommunen er databehandlingsansvarlig for til andre, skal kun gjøres på spesifisert forespørsel og etter samtykke fra registrert person i henhold til relevante lovkrav.
Kommunen skal sikre at pliktige rapporter og meldinger blir sendt til riktig mottaker.
Bruk av personopplysninger i kommunen, skal godkjennes av sikkerhetsleder.
Bruk av personopplysninger som angår ansatte, skal godkjennes av sikkerhetsleder.
Strategi
Alle ansatte som gis tilgang til IT-systemer der det behandles personopplysninger skal autoriseres etter gjeldende rutiner. Autorisasjon skal skje på bakgrunn av dokumentert kompetanse i informasjonssikkerhet, dvs. lest og forstått instruksen **Ansatte og sikkerhetskultur**.

2.4.4 Robusthet

Hovedmål
Vi skal ha sikre IT-systemer som er motstandsdyktige og behandler personopplysninger på en forsvarlig måte og som kan gjenopprette normaltilstand etter en fysisk eller teknisk hendelse.
Delmål:
Det må sikres at kun autorisert personell har adgang til det enkelte fagsystem.
Sensitive personopplysninger sikres mot uautorisert tilgang.
Lagrede personopplysninger sikres gjenopprettet innen rimelig tid.
Strategi
Tilgangskontroll til enkelte fagsystem gjennomføres hvert kvartal.
Sensitive personopplysninger lagres på sikker sone.
Tap av personopplysninger sikres ved hjelp av redundante løsninger og backup.

Områder der personopplysninger databehandles skal sikres med adgangskontroll.
Det skal finnes autorisasjonskontroll til systemer som inneholder personopplysninger.
Alle som skal ha tilgang til områder hvor det behandles personopplysninger, skal signere taushetserklæring.

Det skal etableres prosedyrer for:

- tildeling, sletting og kontroll av autorisasjon, se pkt. 3.6
- tilgang til sensitive personopplysninger for databehandler, se pkt. 4.5
- innsyn, se pkt. 4.8 og 6.0
- anonymisering, se pkt. 3.8
- rapportering og behandling av sikkerhetsbrudd og avvik, se pkt. 10.0

[1] Generelle rettsprinsipper tilsier en tolkning hvoretter hensynet til konfidensialitet antas å gå foran hensynet til tilgjengelighet

- utlevering eller overføring av sensitive personopplysninger, se pkt. 4.4 og 3.7.
- bruk av eksterne tjenesteleverandører, se pkt. 3.4
- gjennomgang og oppfølging av logger, se pkt. 3.11 (nedenfor)
- utfylling og signering av taushetserklæring, se pkt. 3.3
- risikovurderinger se pkt. 8.0

Ekstern datakommunikasjon skal krypteres for sensitive personopplysninger.

2.5 Hovedkravene til informasjonssikkerhet

Informasjonssikkerhet

Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.

Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Internkontroll

Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

Den behandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.

Kongen kan gi forskrift med nærmere regler om internkontroll.»

Eksempler på handlinger som normalt er krenkelser av personvernet:

- At personopplysninger behandles skjult for oss.
- At flere og mer inngående personopplysninger enn nødvendig, samles inn.
- At personopplysninger ikke slettes når det ikke lengre er behov for dem.
- At den registrerte ikke får innsyn i opplysningene om seg selv.
- At personopplysningene som behandles, er feilaktige.
- At personopplysningene tilflyter uvedkommende.

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en enkeltperson.
For eksempel en persons navn, adresseinformasjon og lønn, referanseuttalelser om en person hos et rekrutteringsfirma, oppgavebesvarelser fra skoleelever, klientopplysninger ved krisesentre, skyldneropplysninger i inkassoselskaper, kundeopplysninger i nettbokhandler og klientopplysninger i advokatselskaper. Noen av de nevnte opplysningene vil også være **sensitive** personopplysninger (sensitive personopplysninger).

«Særlige kategorier av opplysninger samt personopplysninger knyttet til straffedommer og straffbare forhold» refererer til definisjoner i peronvernforordningens artikkel 9 og 10:

Sensitive opplysninger/særlige kategorier av personopplysninger:

- rasemessig eller etnisk opprinnelse
- politisk oppfatning
- religiøs eller filosofisk overbevisning
- fagforeningsmedlemskap
- behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person
- helseopplysninger
- opplysninger om en fysisk persons seksuelle forhold eller seksuelle legning

Straffbare forhold:

- personopplysninger i forbindelse med straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak

Sensitive personopplysninger er for eksempel informasjon om hvilke sykdommer en person har hatt, medisiner vedkommende bruker, straffedommer, tidligere og pågående rusmisbruk og seksuell legning.
Årsaken til at det er en egen kategori for sensitive personopplysninger, er at det knytter seg et særlig behov for vern rundt disse. Disse personopplysningene ses normalt på som mer inngripende for den enkelte, og regelverket stiller strengere vilkår for at disse kan behandles. Misbruk eller spredning av slike personopplysninger vil også normalt få større konsekvenser for den enkelte, og det er et behov for ekstra sikring av slike opplysninger.

Det tillattes ikke samtidig behandling av sensitive personopplysninger og bruk av for eksempel kontorstøttesystemer(for eksempel e-post, internett), uten at det etableres tekniske og administrative sikkerhetsløsninger som forhindrer at en bruker uforvarende sender sensitive personopplysninger (for eksempel ved bruk av ”klipp og lim” funksjon mellom ulike programmer).

2.6 Norm for informasjonssikkerhet

Normen for informasjonssikkerhet er et sett med krav til informasjonssikkerhet som er felles for alle aktører i helsesektoren. Normen har spesiell fokus på elektronisk behandling av helse- og personopplysninger, og er juridisk bindende for alle brukere av helsenettet.

Normen ble utarbeidet i 2020, i et samarbeid med flere sentrale aktører i sektoren, blant disse Norsk Helsenett.

Normen er utarbeidet for å sikre tillit til at alle sider ved informasjonssikkerhet i helsesektoren blir tilfredsstillende ivaretatt. Den skal være en veileder for hver enkelt aktør i deres arbeid med informasjonssikkerhet.

Alle brukere av helsenettet er juridisk forpliktet til å følge kravene i denne normen. Dette er en del av avtalen om tilknytning til helsenettet. På denne måten kan vi oppnå større sikkerhet for alle brukere av helsenettet.

Kravene i Normen for informasjonssikkerhet er innarbeidet i sikkerhetshåndbøkene for Melhus kommune.

2.7 Begrunnelse for behandling av personopplysninger

Kommunen har behov for å behandle opplysninger om enkeltpersoner i en rekke sammenhenger for å utføre sine oppgaver. Eksempler er tjenester som ytes til innbyggerne i Melhus kommune i tilknytning til

- Barnehage
- Frivillighetssentralen
- Helse
- Kultur og fritid
- Landbruk
- Pleie og omsorg
- Skole
- Sosiale tjenester
- Tekniske tjenester
- Voksenopplæring

Behandlingene er i hovedsak med hjemmel i lov. Det er i 2020 registrert et trettitalls programmer i kommunen hvor personopplysninger behandles, lagres og formidles. Behandlingene omfatter vanlige og sensitive personopplysninger.

2.8 Ledelsens ansvar

Rådmannen i Melhus kommune er ansvarlig for at lovverket, herunder personopplysningsloven, følges og at internkontroll etableres og følges, og er den behandlingsansvarlige i forhold til personopplysningsloven.

Personvernforordningen stiller krav til den behandlingsansvarliges ansvar. Det innebærer å sette i verk egnede tiltak, både tekniske og organisatoriske, for å sikre og påvise at personopplysninger behandles i samsvar med regelverket (internkontroll)

Rådmannens ansvar omfatter blant annet å

- bestemme formålet med behandlinger av personopplysninger
- påse at behandlingene er lovlige (gyldig behandlingsgrunnlag)
- påse at det er utarbeidet rutiner både for oppfyllelse av Melhus kommunes plikter og de registrertes rettigheter
- utpeke personvernombud

Rådmannen skal videre sørge for at blant annet følgende er på plass;

- Sikkerhetsmål og sikkerhetsstrategi.
- Sikkerhetsorganisasjon.
- Dokumenterte rutiner og tekniske tiltak for oppfyllelse av sikkerhetsstrategi.

Ansvaret omfatter også at det årlig avsettes tilstrekkelige ressurser, både personalmessige og økonomiske, slik at tilfredsstillende informasjonssikkerhet og internkontroll av informasjonssikkerheten opprettholdes.
Rådmannen kan delegere operativt ansvar for daglige arbeidsoppgaver i forbindelse med informasjonssikkerhet og internkontroll, men kan ikke delegere ansvaret i forhold til loven.

2.9 Sikkerhetsmål

Sikkerhetsmålene omfatter ledelsens beslutninger om til hva og hvordan informasjonsteknologien skal benyttes i Melhus kommune for å nå kommunens øvrige mål. Sikkerhetsmål vil således utgjøre en del av Melhus kommunes beskrivelse av sin totale målsetting.

Melhus kommune skal behandle personopplysninger i samsvar med kravene i personopplysningsloven, jf. helseregisterloven og andre særlover for de ulike fagprofesjoner med tilhørende forskrifter. Ingen helse- og personopplysninger skal samles inn, bearbeides, lagres eller slettes uten at den opplysningene omhandler har gitt sitt samtykke, eller det er fastsatt i lov at det er adgang til slik behandling.

Sikkerhetsmålene skal understøtte og sikre Melhus kommunes drift, allmenne tillit og omdømme i det offentlige rom. Dette gjøres ved å forebygge og begrense konsekvensene av uønskede tilsiktede og utilsiktede hendelser internt og eksternt. Sikkerhetsmålene beskriver Melhus kommunes overordnete mål for beskyttelse av kommunens informasjonsbehandling mot interne og eksterne trusler og hendelser av tilsiktet og utilsiktet art.

Følgende 15 sikkerhetsmål er definert:

1. Melhus kommune skal sikre at informasjon behandles iht. krav i relevante lover og forskrifter.
2. Sikkerheten skal ha forankring i ledelsen i Melhus kommune.
3. Sikkerheten skal ivaretas som en integrert del av hele Melhus kommunes organisasjon.
4. Den fysiske sikkerhet ved Melhus kommune skal hindre at uautoriserte får adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.
5. Tilgang til systemer og informasjon gis kun til medarbeidere etter behov.
6. Tilgang til systemer og informasjon for uvedkommende skal forhindres.
7. Melhus kommune skal sikre at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
8. Melhus kommune skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
9. Det skal være mulig å spore uønskede hendelser.
10. Det skal være tatt i bruk rutiner for å håndtere uønskede og virksomhetskritiske hendelser.
11. Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres
12. Det skal forhindres at personer eller systemer i Melhus kommune bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.
13. Melhus kommune skal sikre at medarbeidere som bruker kommunens informasjonssystemer har en tilstrekkelig kompetanse for å ivareta Melhus kommunes sikkerhetsbehov/krav.
14. Melhus kommune skal sikre at personopplysninger som behandles blir ivaretatt på en trygg måte.
15. Personer som ber om det, skal få generell informasjon om Melhus kommunes behandlinger av personopplysninger.

3.0 Sikkerhetsstrategi

Sikkerhetsstrategien vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Sikkerhetsstrategi skal gjøre rede for organisatoriske og tekniske strategiske valg. Sikkerhetsstrategien skal være utformet på en måte som gjør at de ansatte forstår hva ledelsen har bestemt.

Strategien beskriver hvilke virkemidler Melhus kommune velger å bruke for å nå målene ovenfor.
I dette delkapittelet er de ulike strategivalgene oppsummert. En del av områdene er videre utdypet fra delkapittel 3.8 og utover.

Sikkerhetsstrategien dekker følgende områder

1. Organisering
2. Egenkontroll
3. Personell
4. Leverandører
5. Fysisk sikkerhet
6. Tilgang til IT-løsninger
7. Dokumentsikkerhet
8. Endringskontroll
9. Beredskap
10. Avvikshåndtering
11. Systemteknisk sikkerhet (Hefte 3)
12. Anskaffelser av IT-verktøy og IT-løsninger
13. E-post
14. Risikovurderinger (Hefte 3)
15. Ledelsens gjennomgang

3.1 Organisering av sikkerhet

Personopplysningsforskriften (§ 2-7) stiller krav til at det skal bestemmes klare ansvars- og myndighetsforhold for bruk av informasjonssystemer som behandler personopplysninger. Dvs. det *skal besluttes en sikkerhetsorganisasjon og denne skal dokumenteres. Ansvar og myndighet relatert* til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeid (sikkerhetsledelse) må klarlegges.

Operativt ansvar for drift er en utøvende funksjon som omfatter å sikre at informasjonssystemet fungerer som besluttet. Operativt ansvar for å følge opp sikkerhetsarbeidet er en kontrollerende funksjon som omfatter etterprøving av at informasjonssystemet benyttes som besluttet. Sikkerhetsorganisasjonen skal forvalte og styre organiseringen av sikkerhetsarbeidet, og bør baseres på tverrfaglig samarbeid.

Med dette som utgangspunkt har Melhus kommune etablert en sikkerhetsorganisering som består av følgende funksjoner:

- Rådmann (behandlingsansvarlig)
- Kommunalsjef, enhetsleder, systemeier og systemansvarlig
- Sikkerhetsleder
- Personvernombud
- Arkivleder
- Leder med personalansvar
- Bruker/medarbeider
- IKT-drift/databehandler

Med sikkerhetsorganisering menes oppgaver og ansvar med betydning for informasjonssikkerheten og ikke en egen organisasjon. Nevnte funksjoner skal ivareta sikkerhetsansvaret som en del av sitt totale ansvar.

Funksjonsbeskrivelser[2]

Rådmannen

er databehandlingsansvarlig for all behandling av personopplysninger herunder ansvarlig for å bestemme formålet med databehandlingene og ha dokumentert oversikt over disse:

[2] Funksjonsbeskrivelsene er begrenset til sikkerhetsmessige aspekter.

Dataansvarlig er den som alene eller sammen med andre virksomheter bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke midler som skal benyttes.

I personvernforordningen benyttes begrepet behandlingsansvarlig, som er det samme som dataansvarlig i helsesektoren.

Dataansvarlig

- har det overordnede ansvar for informasjonssikkerheten og skal sikre at tjenester er tilgjengelig for å gjennomføre tiltak
- har ansvar for at styringssystemet for informasjonssikkerhet blir implementert og vedlikeholdt
- har ansvar for at det fastsettes akseptabelt risikonivå og gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig (jf. kap. 3)
- skal sikre den registrertes rettigheter (jf. kap. 4)
- skal etablere og dokumentere tekniske og organisatoriske tiltak (jf. kap. 5)
- skal håndtere avvik (jf. kap. 5.8)

Dataansvarlig er ansvarlig for å opptre i henhold til personvernprinsippene. Dette innebærer at personopplysninger skal (jf. kap. 2.1):

- behandles på en lovlig måte (gyldig behandlingsgrunnlag)
- behandles på en rettferdig måte (med respekt for de registrertes interesser og rettigheter)
- behandles på en åpen måte (oversiktlig, forutsigbar og forståelig informasjon) med hensyn til den registrerte (brukeren)
- bare registreres for bestemte formål som skal være legitime
- bare benyttes til de formål de er registrert for, med mindre det finnes behandlingsgrunnlag for andre formål
- være relevante, adekvate, korrekte og om nødvendig oppdaterte for de formål de er registrert for
- lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene
- sikres mot uautorisert tilgang, endring, ødeleggelse og spredning

Kommunalsjef, enhetsleder, systemeier og systemansvarlig
har ansvar for å stille krav til konfidensialitet, integritet, tilgjengelighet, robusthet og kvalitet for det system vedkommende er systemeier for, slik at det oppfyller lovbestemte og andre krav:

- definerer tilgangsroller for sitt system innenfor rammene gitt av AD og gjøre disse kjent
- skal sørge for at det inngås skriftlige avtaler med IKT-leverandør/databehandler med krav til tjenestenivå og forvaltning
- skal sørge for at nødvendig opplæring blir gitt
- overvåker risiko forbundet med informasjonsbehandling og å forestå risikovurdering ved behov

Sikkerhetsleder
Har det utøvende ansvar for Melhus kommunes sikkerhetsarbeid samt å forberede ledelsens årlige gjennomgang og følge opp iverksetting av tiltak som er besluttet.

- lage årlig revisjonsplaner og forestå gjennomføring av sikkerhetsrevisjoner
- vurdere og rapporterte avvik og meddele avvik til kommunens ledelse i samsvar med rutine for avviksbehandling
- forestå gjennomføring av risikovurderinger
- drive opplysningsvirksomhet om informasjonssikkerhet

- være rådgiver i sikkerhetsspørsmål
- utvikle og vedlikeholde overordnede styrende dokumenter
- iverksette og delta i revisjoner, risikovurderinger og egenkontroll
- avgjøre om nye løsninger eller endringer er innenfor akseptabelt risikonivå
- stille krav til nye/endrede sikkerhetsløsninger ved IKT drift, både for etablerte og nye behov som oppstår ved at nye IKT-løsninger innføres
- påse at avvikshåndtering, forbedringsprosesser og vedlikehold av informasjonssikkerheten gjøres i alle ledd, herunder om nødvendig å gi pålegg
- iverksette korrektive og andre sikkerhetsrelaterte tiltak

Personvernombud
Personvernombudets hovedoppgave er å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen til den behandlingsansvarlige eller databehandleren, samt til de ansatte som utfører behandlingen av personopplysninger:

- Kontrollere overholdelsen av personvernregelverket
- Gi råd om vurdering av personvernkonsekvenser (DPIA)
- Samarbeid med Datatilsynet og funksjon som kontaktpunkt
- Bidra til å få oversikt over behandlingene i virksomheten

Leder med personalansvar
Enhver leder er ansvarlig for informasjonssikkerhet innen egen organisasjonsenhet. Ledere skal sørge for at underlagte enheter og ansatte der det er relevant:

- er kjent med og etterlever sitt ansvar, kommunens styringssystem for informasjonssikkerhet og sikkerhetsbestemmelser som er relevante
- gjennomfører tilstrekkelig sikkerhetsopplæring av eget og innleid personell, slik at disse har en forståelse av hva som er forventet av dem
- innhenter taushetserklæringer for alle ansatte og innleid personell og påser at disse er kjent med og etterlever styrende dokumenter som regulerer brukeratferd
- tildeler og kontrollerer personellets tilgang til informasjon etter fastsatt tilgangsregime
- rapporterer og formaliserer registre, prosjekter og øvrige databehandlinger inneholdende person- og helseopplysninger iht. kommunens rutiner
- følger opp det daglige sikkerhetsarbeidet gjennom et etablert system for avviksbehandling, nødvendige kontroller og iverksette relevante tiltak
- er ansvarlig for resultater, fremdrift og rapportering av sikkerhetsarbeidet innen eget ansvarsområde
- er ansvarlig for at beredskapsplaner ved bortfall av informasjonssystemer finnes

Bruker/medarbeider:
Den enkelte medarbeider er ansvarlig for å:

- følge Melhus kommunes sikkerhetsbestemmelser
- ha en forståelse av hva som er forventet av dem (atferd)
- søke informasjon ved usikkerhet eller tvil
- forhindre eller rapportere hendelser som kan innebære avvik
- rapportere avvik når disse oppstår til nærmeste leder eventuelt sikkerhetsleder

Enhver ansatt oppfordres til å bidra aktivt med synspunkter og komme med forslag til forbedringer knyttet til sikkerhet.

IKT-drift/databehandler
IKT-drift/databehandler har ansvar for at kommunens informasjonssystem er tilgjengelig og at det oppfyller lovbestemte og andre krav samt fungerer som besluttet. Dette inkluderer å

- overvåke risiko forbundet med informasjonsbehandling og forestå risikovurderinger ved behov
- utarbeide beredskapsplan for IKT-området
- følge opp partnere, leverandører og andre databehandlere som har betydning for informasjonssikkerheten
- håndtere meldte avvik
- å sørge for at bruk av personopplysninger begrenses til det som er avtalt
- sørge for å utvikle og etterleve driftsdokumentasjon
- sørge for å utvikle og etterleve dokumentasjon for konfigurasjons- og endringskontroll
- å etablere tiltak for å hindre uautorisert bruk og adgang til informasjonssystemene
- å etablere tiltak for å registrere sikkerhetsavvik, hindre forsøk på uautorisert bruk og tilhørende avvikshåndtering
- å etablere tiltak for å motstå angrep fra ondsinnet programvare

3.2 Egenkontroll

Melhus kommune skal ha rutiner for kontroll av at rutiner for håndtering av personopplysninger og for kontroll av informasjonssikkerhetstiltak er i bruk og fungerer etter hensikten.
Sikkerhetsleder er ansvarlig for at egenkontrollskjema blir oppdatert etter ledelsens gjennomgang og forøvrig ved behov som følge av avviks- og endringshåndtering.

Resultatene fra egenkontrollene og fra andre områder, inngår i ledelsens årlige gjennomgang av informasjonssikkerhet.
Egenkontroll er nærmere beskrevet i IT-løsning - drift pkt. 7.0.

3.3 Personell og sikkerhet

Det vises til uttømmende behandling av temaet i heftet **Ansatte og sikkerhetskultur**.

3.4 Partnere og leverandører

Eksterne partnere og leverandører til Melhus kommune skal forplikte seg gjennom avtale til å følge relevante krav i lovgivningen (personopplysningsloven med forskrift og annen, relevant lovgivning). Videre vil kravene i styringssystem for sikkerhet være gjeldende.

Leverandørers ansatte som har oppdrag i Melhus kommune og som får tilgang til IT-tjenestene, skal underskrive egen autorisasjon og taushetserklæring, jf. **vedlegg 4.**

Det vises ellers til eget kapittel i **IT-løsninger-drift** om Sikkerhetsregler for eksterne brukere av IKT-tjenester fra Melhus kommune.

3.5 Fysisk sikkerhet

Se egen omtale i pkt. 11.0

3.6 Tilgang til IKT-løsninger

Virksomhetsleder er ansvarlig for å klarlegge og autorisere en ansatts behov for tilgang og formidle dette til IKT-seksjonen ved ansettelse eller endringer i ansvar.

Virksomhetsleder er ansvarlig for å melde til IT-seksjonen at personell slutter slik at tilgangsrettigheter fjernes.

IKT-seksjonen er ansvarlig for å vedlikeholde tilgangsrettigheter samt holde oversikt over de tilgangsrettigheter som er gitt.

3.7 Dokumentsikkerhet

Alle dokumenter og lagringsmedia som inneholder beskyttelsesverdig informasjon, skal oppbevares, forsendes og destrueres på en slik måte at det ikke kommer uvedkommende i hende.

Med beskyttelsesverdig forstås her informasjon som er underlagt krav om beskyttelse gjennom regelverk (for eksempel personopplysningloven) eller informasjon med særlig behov for beskyttelse (for eksempel informasjon som blir ansett som samfunnskritisk eller virksomhetskritisk).

Dokumenter som inneholder sensitive opplysninger skal registreres og lagres i sikker sone. Der det ikke er tilgang til å lagre i sikker sone, må dokumentet lagres i eget fysisk arkiv.

Dersom beskyttelsesverdig informasjon skal transporteres utenom kommunens IKT-system, skal denne anonymiseres og sendes som rekommandert post. Det skal utarbeides Databehandleravtale, se punkt 6.0. I denne skal det bl.a. gå fram hvordan informasjonen skal behandles, sletting av informasjon og at informasjonen ikke brukes til andre formål.

3.8 Endringskontroll

Ved endringer i Melhus kommunes informasjonssystemer skal alltid beskyttelsesbehov vurderes, og om endring kan ha konsekvenser for sikkerheten.

Endringer som kan ha konsekvenser for informasjonssikkerheten, skal godkjennes av sikkerhetsleder.

For endringer som kan ha sikkerhetsmessig konsekvens, skal IKT-seksjonen utarbeide en risikovurdering inkludert forslag til tiltak som oversendes sikkerhetsleder som en del av endringsforespørsel.

Sikkerhet skal være et vurderingspunkt gjennom alle faser av en endring.

Krav til sikkerhet og overordnet vurdering av risiko skal inngå i eventuelle forprosjekt.

Ved en eventuell kontrakt med tredjepart skal krav til sikkerhet inngå i kontrakten.

Produksjonsdata som inneholder sensitive personopplysninger skal anonymiseres før de benyttes ved tester knyttet til endringer, se ellers punkt 3.7 siste avsnitt.

Sikkerhetsnivå skal verifiseres før endringer settes i drift.

3.9 Beredskap

Melhus kommune har en beredskapsordning hvor ansatte i IKT-seksjonen arbeider i en turnusordning slik at kommunen, rent driftsmessig, har tilgjengelig IKT-kompetanse i den ordinære arbeidstiden.
Det er videre satt opp en beredskapstelefon slik at brukerstøtte kan nås i ordinær arbeidstid.

3.10 Avvikshåndtering

Se om avvikshåndtering i pkt. 10.0.

3.11 Systemteknisk sikkerhet

Systemteknisk sikkerhet er beskrevet i IT-løsning-drift.

3.12 Anskaffelse av fagsystemer og annen virksomhetskritisk programvare

For fagsystemer og annen virksomhetskritisk programvare gjelder:

Ansvaret for håndtering av sikkerhetsbehov i det enkelte fagsystem ligger hos virksomhetsleder.
Utøvende ansvar kan delegeres til systemansvarlig for fagsystemet eller andre navngitte personer.

All programvare skal anskaffes eller utvikles på bakgrunn av detaljerte kravspesifikasjoner der også krav til sikkerhet inngår.

Teknisk sikkerhetsnivå skal verifiseres i alle prosjektets faser ved utvikling og anskaffelse.

Før programvaren/systemer settes i produksjon, skal teknisk sikkerhetsnivå verifiseres. Ved feil eller mangler, skal retting av eventuelle feil/mangler gjennomføres før systemet settes i produksjon. Rettelser av feil og mangler skal verifiseres.

Før programmer eller systemer settes i produksjon skal rutiner for drift, proaktiv overvåkning og beredskap være iverksatt.

Verifikasjon av sikkerhet gjennom test skal utføres av andre personer enn de som har vært med på å utvikle systemet eller personer som drifter systemer.

Sikkerhetsleder har ansvaret for selve gjennomføringen av testen og formidler resultatene tilbake til prosjektet.

3.13 E-post

Se hefte 1, Ansatte og sikkerhetskultur pkt. 3.7 om bruk av e-post og hefte 2 Policy, regelverk, rutiner og prosedyrer pkt. 4.9 om innsyn i e-post.

4.0 Risikostyring

Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere kommunen med hensyn til risiko. Det omfatter å få oversikt over informasjon og teknologi i virksomheten, identifisere trusler og mulige uønskede hendelser for både virksomheten og de registrerte, analysere risikoen og etablere tiltak for å opprettholde nivå for akseptabel risiko.

Melhus kommune skal etablere tekniske og organisatoriske tiltak som er egnet for å håndtere risiko på en tilfredsstillende måte. Dette inkluderer å sikre både konfidensialitet, integritet, tilgjengelighet og robusthet i informasjonssystemene. Disse hensynene skal balanseres.

Det skal tas hensyn til den tekniske utviklingen, gjennomføringskostnader og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i, når et akseptabelt risikonivå vurderes. Arbeidet med risikostyring skal ta hensyn til for eksempel type og mengde opplysninger, virksomhetens størrelse og behandlingens kompleksitet.

4.13 Risikovurdering

Melhus kommune skal gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i informasjonssystemet eller endringer i trusselbildet.

Risiko betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse.

Risikovurderingen baseres på blant annet personopplysningsforskriften § 2-1, Forholdsmessige krav om sikring av personopplysninger. Opplysninger av ulike typer/kategorier skal beskyttes "godt nok". Beskyttelsestiltak koster penger og innsats samt reduserer ofte tilgjengelighet.

Formålet med risikovurdering er å undersøke hvorvidt den risiko som avdekkes er innenfor de akseptkriterier Melhus kommune har fastlagt. Risikovurderingen danner grunnlag for iverksetting av

nødvendige sikkerhetstiltak, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten.

4.2 Forholdsmessighet ved valg av tiltak

Ved valg av egnede tekniske og organisatoriske tiltak skal tiltakene vurderes opp mot virksomheten, art og omfang for behandling av personopplysninger, brukersikkerhet, risikobildet mv.

Dette gjelder særlig i vurderingen av egnet sikkerhetsorganisasjon, arbeidsoppgaver, kontrolloppgaver og tiltak innen informasjonssikkerhet (for eksempel tilgangsstyring, logging, fysisk sikring, beredskap mv.).

Virksomheten skal sørge for at det er forholdsmessighet mellom risiko og tiltakets kostnad.

4.3 Akseptkriterier

I Melhus kommune er akseptkriteriene som følger:

4.3.1 Konfidensialitet:

Indikator:

Antall avvik hvor person- og/eller helseopplysninger er blitt utleverte til uautoriserte.
Antall personer som har fått uautorisert tilgang til opplysningene.

Akseptkriterier:

Sensitive personopplysninger om innbygger/bruker eller ansatt skal alltid gis til rett person – null toleranse.
Utilsiktet utlevering av sensitive personopplysninger om innbygger/bruker skal hindres med tekniske tiltak og kompetansemessige tiltak.
Uautorisert tilgang til sensitive personopplysninger om innbygger/bruker skal hindres med tekniske og kompetansemessige tiltak.

4.3.2 Integritet/kvalitet:

Indikator:

Antall avvik der det er oppdaget brudd på integritet som har opphav i feil eller mangler ved informasjonssystemer eller pga. menneskelige feil

Akseptkriterier:

Feil behandling av innbygger/bruker eller ansatt som følge av feil i data (personopplysninger ikke korrekte eller ufullstendige) skal ikke forekomme - null toleranse.
Feil i personopplysninger skal hindres med tekniske tiltak, med gode rutiner og god opplæring.

4.3.3 Tilgjengelighet/Robusthet:

Indikator:

Antall tilgjengelighetsbrudd i virksomhetskritiske IT-systemene målt fra sluttbruker.
Tilgjengelighetsbrudd omfatter også responstid ut over angitt krav.
Nedetid på virksomhetskritiske IT-systemer. Det skilles mellom planlagt og ikke-planlagt nedetid

Akseptkriterier:

Ikke-planlagte avbrudd:
Antall ikke-planlagte avbrudd i virksomhetskritiske systemer skal ikke overstige 1 pr. måned og ikke mer enn tre ganger pr. år i det enkelte system. Avbruddets varighet skal ikke overstige 15 minutter i tidsrommet 0700 – 1800 mandag – fredag og 1 time i tidsrommet 1800 - 0700 hverdager og i helger (målt hos bruker).

Planlagte avbrudd:
Antall planlagte avbrudd i virksomhetskritiske systemer skal gjennomføres i avtalt servicevindu og ikke overstige 1 pr. måned. Avbruddets varighet skal ikke overstige 4 timer og gjøres i tidsrommet 2200 – 0700 (målt hos bruker).
Planlagte avbrudd i de enkelte virksomhetskritiske kritiske systemer ut over 4 timer pr. måned (målt hos bruker) skal ikke overstige 2 pr år. Utover dette skal det avtales i hvert enkelt tilfelle.
Varsling til bruker ved planlagt avbrudd i kritiske systemer skal skje minimum 14 dager på forhånd.

Responstid:
Responstid skal ikke overstige definerte krav for virksomhetskritiske system. Krav til responstid skal nedfelles i avtaleverket for hver enkelt applikasjon.
Responstid som overskrider definerte krav, defineres som uplanlagt nedetid

Melhus kommunes ledelse har ansvar for iverksetting av risikovurdering. Resultat fra analysen rapporteres til Melhus kommunes ledelse, se pkt. 12.

4.5 Vurdering av personvernkonsekvenser (DPIA)

Virksomheter skal alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte. Virksomheten skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering, også kalt DPIA14.

Personvernkonsekvensvurderingen skal gjøres før behandlingen av personopplysninger starter.

Høy risiko for personvernet kan oppstå:

- når personopplysninger behandles i stor skala
- ved bruk av ny teknologi
- når personopplysninger behandles på en automatisert, systematisk og omfattende måte, og dette danner grunnlag for avgjørelser som har rettsvirkning eller påvirker den registrerte i betydelig grad
- dersom behandlingens art, omfang, formål og sammenhengen den utføres i, tilsier det

Datatilsynet har laget en liste over behandlingsaktiviteter som alltid krever at det gjennomføres en personvernkonsekvensvurdering.

Personvernkonsekvensvurdering skal minst inneholde:

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger
- beskrivelse av formålet med behandlingen av personopplysninger
- en vurdering av om behandlingene av helse- og personopplysninger er nødvendige og står i rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

Den behandlingsansvarlige skal rådføre seg med personvernombudet i forbindelse med utførelsen av en personvernkonsekvensvurdering.

Det skal planlegges tiltak som reduserer risikoen for personvernet. Dersom behandlingen av personopplysninger medfører en høy risiko som ikke kan reduseres ved hjelp av rimelige tiltak, skal den dataansvarlige be om forhåndsdrøftelse med Datatilsynet før behandlingen av opplysningene starter.

5.0 Sikring av personopplysninger

5.1 Protokoll over behandlingsaktiviteter

Melhus kommune skal ha en protokoll over hvilke behandlinger av personopplysninger som foretas, og hvilke opplysninger som inngår i disse. Protokollen er sentral for at Melhus kommune skal være i stand til å ivareta pliktene sine. Protokollen danner også grunnlag for utarbeidelse av Melhus kommunes sikkerhetsmål og sikkerhetsstrategi, og vil være underlag ved risikovurderinger.
Protokoll over behandlinsaktiviteter.doc

For annen informasjon som behandles elektronisk i den enkelte enhet, må man følge det lov- og regelverk som er relevant for den enkelte informasjonskategori, i hovedsak offentlighetslov, forvaltningslov og eventuelle særlover og tilhørende regelverk.

Prorokollen over behandlingsaktiviteter skal gi kortfattet informasjon om:

- System/dataeier
- Funksjonsområde/ansvarlig
- Databehandler
- Formålet med behandlingen?
- Behandlingsgrunnlag
- Hvilken lovhjemmel ligger til grunn for behandling av personopplysningene?
- Kategorier av registrerte og personopplysninger
- Er personopplysningene sensitive, (personopplysninger av særlige kategorier).
- Tekniske og organisatoriske sikkerhetstiltak
- Personvernkonsekvensvurdering/ROS
- Tidsfrist for sletting/planlagt lagringstid
- Kort om hvordan programmet brukes

5.2 Formål med behandling av personopplysninger

Fastsette formål

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål
Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at alle berørte har samme entydige forståelse av hva personopplysningene skal brukes til. At formålet skal være legitimt innebærer at det i tillegg til å ha et rettslig grunnlag også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer.

Før ei verksemd set i gang med å behandle personopplysningar, må det liggje føre eit eller fleire klart formulerte formål.

Ei verksemd kan aldri samle eller lagre personopplysningar utan eit formål. Dette vert slått fast i eit av personvernprinsippa i personvernforordninga. Personopplysningar skal berre nyttast for spesifikke, uttrykkelege, angitte og legitime formål.

Det at opplysningane kan vise seg å komme til nytte ein dag, er ikkje eit godt nok formål. Verksemda må ha eit reelt formål med opplysningane, og det må vere klart uttrykt og bestemt på førehand. Dette inneber at dersom verksemda ønskjer å bruke personopplysningar, må ho starte med å formulere formålet skriftleg først.

Når ein skal formulere formålet, er det viktig å vere konkret og open. Vide eller vage formuleringar er ikkje tillatne. Verksemda har plikt til å gje den einskilde informasjon om formålet med behandlinga av personopplysningar på ein forståeleg måte.

5.3 Behandlingsgrunnlag

All behandling av personopplysninger må ha et rettslig grunnlag for å være lov. Det betyr at virksomheten på forhånd må ha identifisert om det finnes et behandlingsgrunnlag. Hvis ikke det finnes, er behandlingen ulovlig

5.3.1 Vanlige personopplysninger

Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

- den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,
- behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,
- behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,
- behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,
- behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,
- behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

5.3.2 Særlige kategorier av personopplysninger (sensitive personopplysninger)

I utgangspunktet er det forbudt å behandle visse kategorier av personopplysninger. Mange omtaler disse opplysningstypene som sensitive personopplysninger.

De kategoriene av opplysninger dette gjelder er:

Sensitive opplysninger/særlige kategorier av personopplysninger:

- rasemessig eller etnisk opprinnelse
- politisk oppfatning
- religiøs eller filosofisk overbevisning
- fagforeningsmedlemskap

- behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person
- helseopplysninger
- opplysninger om en fysisk persons seksuelle forhold eller seksuelle legning

Straffbare forhold:

- personopplysninger i forbindelse med straffedommer og straffbare forhold eller tilknyttede sikkerhetstiltak

Det finnes imidlertid mange unntak fra forbudet. Lovens system er at det må foreligge **et særskilt grunnlag i tillegg til behandlingsgrunnlag** for å behandle denne typen opplysninger.

- Den registrerte har gitt uttrykkelig samtykke.
- Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle og utøve sine arbeidsrettslige, trygderettslige og sosialrettslige plikter og rettigheter i den grad behandlingen er tillatt etter lov eller tariffavtale.
- Behandlingen er nødvendig for å verne den registrertes eller en annen persons vitale interesser hvis den registrerte ikke er i stand til å gi samtykke.
- Behandlingen utføres av en stiftelse, sammenslutning eller ideelt organ som har mål av politisk, religiøs eller fagforeningsmessig art, så lenge det er snakk om personopplysninger om medlemmer og liknende, det foreligger nødvendige garantier og opplysningene ikke utleveres uten samtykke.
- Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort.
- Behandlingen er nødvendig i forbindelse med rettskrav eller domstolene handler innenfor rammen av sin domsmyndighet.
- Behandlingen er nødvendig av hensyn til viktige allmenne interesser og har hjemmel i lov.
- Behandlingen er nødvendig i forbindelse med forebyggende medisin, medisin i arbeidslivet, vurdering av en arbeidstakers arbeidskapasitet, medisinsk diagnostikk, ytelse av helse- eller sosialtjenester, sosialfaglig eller medisinsk behandling eller forvaltning av helse- eller sosialtjenester og -systemer. Dette gjelder imidlertid bare dersom opplysningene behandles av en fagperson underlagt taushetsplikt, og behandlingen av personopplysninger må ha hjemmel i lov eller følge av avtale med helsepersonell.
- Behandlingen er nødvendig av allmenne folkehelsehensyn.
- Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål, på visse betingelser og under forutsetning av at behandlingen har hjemmel i lov.

Der forordningen sier at en behandling av personopplysninger krever hjemmel i lov, stiller den også visse krav til loven eller ting loven skal inneholde. Det vil si at en hvilken som helt lovhjemmel i seg selv ikke nødvendigvis er tilstrekkelig.

De ulike behandlingene som er identifisert, må vurderes mot aktuelle behandlingsgrunnlag.
Hvis en av behandlingene ikke faller innenfor eksisterende behandlingsgrunnlag, må Melhus kommune avvikle behandlingen eller sørge for at det etableres et behandlingsgrunnlag, eksempelvis ved innhenting av samtykke.

Det skal føres oversikt over alle behandlingsaktiviteter som omfatter personopplysninger, inkludert oversikt over behandlingsgrunnlaget for slik behandling. ..\..\Elektroniske dataregistre\Oversikt over behandling av personopplysninger.docx

Den registrerte skal informeres om sine rettigheter til innsyn, retting og sletting av personopplysningene. For retten til sletting må dette vurderes om annet er grunngitt i lov.

5.4 Personvernombud

Behandlingsansvarlige og databehandlere skal utpeke personvernombud dersom behandlingen utføres av en offentlig myndighet eller et offentlig organ. Ombudet har som oppgave å bidra til at den behandlingsansvarlige følger personopplysningsloven med forskrift.

Virksomheten skal sikre at personvernombudet ikke mottar instrukser om utførelsen av oppgavene sine, hverken fra den behandlingsansvarlige eller andre. Dette innebærer at ombudet ikke skal få instrukser om hva utfallet av en sak som er til vurdering hos ombudet skal være, hvordan ombudet skal undersøke en klage, eller hvorvidt ombudet skal rådføre seg med Datatilsynet. Ombudet skal heller ikke instrueres i sitt syn på regelverket, slik som for eksempel hvordan en personvernregelverket skal tolkes.

6.0 Behandling av personopplysninger - gjennomførende dokumentasjon

Melhus kommune skal ha rutiner for iverksettelse og opphør av behandling av personopplysninger. Det skal for den enkelte behandling av personopplysninger etableres rutiner for:

1. Iverksettelse og opphør av behandling,
2. Overholdelse av melde- og eventuell konsesjonsplikt,
3. Sletting av personopplysninger,
4. Utlevering av personopplysninger til andre,
5. Kvalitetssikring av personopplysninger,
6. Innhenting og kontroll av samtykke,
7. Oppfyllelse av plikt til informasjon,
8. Innsyn, retting og supplering,
9. Innsyn i e-post og private filområder
10. Ny behandling

6.1 Iverksettelse eller opphør av behandling

Følgende er elementer i rutine for iverksettelse av behandling:

- Vurdere behov for ny behandling av personopplysninger.
- Vurdere formål mot behandlingsgrunnlag.
- Vurdere type opplysninger.
- Gjennomføre risikovurdering.
- Gjennomføre nødvendige sikkerhetstiltak.
- Utarbeide rutiner eller oppdatere rutiner.

Følgende er elementer i rutine for opphør av behandling og må konkretiseres av den ansvarlige:

- Kontroller at oversikten over opplysninger stemmer.
- Er det grunnlag for videre oppbevaring med et nytt behandlingsgrunnlag?

- Slette lagrede relaterte personopplysninger.

6.2

6.3 Sletting av personopplysninger

Krav til sletting av personopplysninger er beskrevet i § 28 i personopplysningsloven.

Bestemmelsen forbyr lagring av unødvendige personopplysninger. Bestemmelsen slår fast at "den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes."

Vær oppmerksom på at en særlov kan gi andre regler for sletting.

Melhus kommune skal ha rutiner for sletting av personopplysninger som det ikke er nødvendig å lagre lenger. Krav til sletting kan inntreffe på grunn av en organisatorisk endring, f.eks. bortfall av formål eller på grunn av at et tidskrav for lagring utløper. Det kan være grunner relatert til historiske, statistiske eller vitenskapelige formål som åpner for lengre lagring under visse forutsetninger. Se nevnte paragraf for detaljer.

Følgende er elementer i rutine for sletting av personopplysninger og må konkretiseres av den behandlingsansvarlige:

- Vurdere krav til sletting av personopplysninger ved endringer i tjenester som ytes av Melhus kommune, ved endringer i organisering og ved endringer av informasjonssystemer.
- Vurdere krav til sletting av personopplysninger månedlig basert på oversikt over opplysninger og lagringstid.
- Behandlingsansvarlig har ansvar for godkjenning av sletting av utvalgte opplysninger.
- Godkjenne sletting av utvalgte opplysninger i alle kopier.
- Verifisere sletting ved kontroll av logger for sletting av opplysninger i alle kopier.

6.4 Utlevering av personopplysninger til andre behandlingsansvarlige

Dette kapitlet omfatter rutiner for utlevering av personopplysninger til andre behandlingsansvarlige. Utleveringen er i seg selv en ny behandling som krever behandlingsgrunnlag (hjemmel) etter personopplysningsloven. Dersom ikke annet behandlingsgrunnlag finnes, må den behandlingsansvarlige som ønsker å utlevere data, ha samtykke fra de(n) registrerte for å utlevere opplysningene.
Utlevering omfatter ikke bruk av eksisterende personopplysninger til ny behandling innenfor samme virksomhet. I dette tilfellet må man sørge for et behandlingsgrunnlag.
Utlevering omfatter heller ikke oversendelse av personopplysninger til databehandlere.
Utlevering etter dette kapitlet omfatter ikke innsyn i egne personopplysninger. Innsyn er behandlet nedenfor.
Følgende er elementer i rutine for utlevering av personopplysninger og må konkretiseres av den behandlingsansvarlige:

- Virksomhetsleder kan delegere myndighet til leder eller medarbeider i Melhus kommune som skal godkjenne utlevering av personopplysninger. Dersom dette ikke er gjort, skal kun

virksomhetsleder selv godkjenne utlevering. Slik delegering av myndighet skal være dokumentert.

- Det skal bestemmes hvem som skal utføre oppgaven, eventuelt oppgavene, i forbindelse med utlevering.

- På forespørsel om utlevering skal det vurderes om forespurte personopplysninger kan utleveres. Som ved andre behandlinger, skal utleveringen være formålsbestemt og tilfredsstille krav til behandlingsgrunnlag i personopplysningslovens § 8 eller § 9 (inkl. § 8).

6.5 Kvalitetssikring av personopplysninger

Opplysningene skal holdes korrekte og oppdaterte i forhold til formålet med behandlingen (personopplysningsloven § 11).

6.6 Innhenting og kontroll av samtykke

Behandling av personopplysninger bør i størst mulig utstrekning basere seg på samtykke fra den registrerte. Dette gir godt personvern ved at den registrerte har bedre kontroll med egne opplysninger. Samtykket må være frivillig, uttrykkelig og informert, jf. personopplysningsloven § 2 nr. 7. Loven stiller ingen formkrav til samtykket, men Datatilsynet anbefaler at det innhentes skriftlig. Skriftlighet vil lette bevisproblemer i situasjoner hvor det reises tvil om hva den registrerte har samtykket til.
Et samtykke kan trekkes tilbake når som helst.

6.7 Oppfyllelse av plikt til informasjon

Den behandlingsansvarlige er pålagt å informere den registrerte om behandlingen før den tar til (personopplysningsloven §§ 19 og 20). Informasjon skal gis av eget tiltak, uten at den registrerte krever det, og uten kostnader for den registrerte, jf. personopplysningsloven § 17.

6.8 Innsyn, retting og supplering

Innsyn
Rett til innsyn i personopplysninger er beskrevet i personopplysningsloven § 18 (se også vedlegg 3-Personvernerklæring):
"Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:
a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,
c) formålet med behandlingen,
d) beskrivelser av hvilke typer personopplysninger som behandles,
e) hvor opplysningene er hentet fra, og
f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om
a) hvilke opplysninger om den registrerte som behandles, og
b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a - f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

Retten til informasjon etter annet og tredje ledd gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte."

Plikt til å informere når det samles inn opplysninger fra den registrerte er beskrevet i personopplysningsloven § 19:
"Når det samles inn personopplysninger 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 best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28.
Varsling er ikke påkrevd dersom det er på det rene at den registrerte allerede kjenner til informasjonen i første ledd."

Plikt til å informere når det samles inn opplysninger fra andre enn den registrerte, er beskrevet i personopplysningsloven § 20:
"En behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, skal av eget tiltak informere den registrerte om hvilke opplysninger som samles inn og gi informasjon som nevnt i § 19 første ledd så snart opplysningene er innhentet. Dersom formålet med innsamling av opplysningene er å gi dem videre til andre, kan den behandlingsansvarlige vente med å varsle den registrerte til utleveringen skjer.
Den registrerte har ikke krav på varsel etter første ledd dersom

a) innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov,
b) varsling er umulig eller uforholdsmessig vanskelig, eller
c) det er på det rene at den registrerte allerede kjenner til informasjonen varslet skal inneholde.
Når varsling unnlates med hjemmel i bokstav b, skal informasjonen likevel gis senest når det gjøres en henvendelse til den registrerte på grunnlag av opplysningene."

Melhus kommune skal ha rutine for behandling av forespørsel om innsyn fra registrert.
Følgende er elementer i rutine for behandling av forespørsel om innsyn og må konkretiseres av den behandlingsansvarlige:

- Mottak av forespørsel om innsyn for mulig registrert person.
- Eventuelt be om skriftlig bekreftelse på forespørsel.
- Formidling av forespørselen til aktuelle system- eller dataeiere.
- Melding til forespørrer dersom forespørselen ga negativt resultat.
- Dersom forespørrer er registrert; skrive ut eventuelt utarbeide i henhold til intern rutine, informasjon fra aktuelle systemer som spesifisert i personopplysningsloven
- §18, a) - f).
- Samle informasjon fra aktuelle systemer og oversende til den som forespør.

Retting og supplering
Personopplysninger skal være tilstrekkelige og relevante for formålet med behandlingen (personopplysningsloven § 11). Kravet til relevans trekker opp en ytre grense for hvilke personopplysninger som kan tas med i behandlingen, og kan ikke fravikes gjennom samtykke fra den registrerte. Kravet til tilstrekkelighet innebærer at man må ha nok opplysninger for å kunne ivareta formålet med behandlingen.

Melhus kommune skal ha rutine for behandling av forespørsel om retting og supplering av registrert.

Det kan også være behov for retting i henhold til lovens § 27. Bestemmelsen slår blant annet fast: "Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene."

Melhus kommune skal også ha rutine for retting når det avdekkes feil internt i kommunen.
Den behandlingsansvarlige skal da gjennomføre følgende prosedyre:

- Registrere forespørsel om retting eller supplering.
- Formidle forespørsel til aktuelle system-/dataeiere.
- Verifisere korrekthet av forespurte endringer av opplysninger.
- Utstede arbeidsordre for oppdatering av system(er).
- Bekrefte skriftlig til den som forespurte om endringer som er gjort.

6.9 Innsyn i e-post og private filområder

I utgangspunktet er det ikke adgang for arbeidsgiver til å gjøre innsyn i ansattes personlige e-postkasse og filer på personlige filområder. For e-post forutsetter dette at den ansatte har e-postadresse med eget navn eller initialer ved Melhus kommune eller annen adresse ved Melhus kommune som bare disponeres av henne.

Regler om innsyn i ansattes e-post er nærmere beskrevet her:
http://datatilsynet.no/Sektor/Arbeidsliv/Innsyn-i-ansattes-e-post/

I Melhus kommune gjelder følgende rutine:
Arbeidstakeren skal varsles før innsyn. Disse tre punktene skal i tillegg gjennomføres:
1. Arbeidstakeren må få tilbud om å være tilstede ved åpningen selv, eller selv få utpeke en representant som kan være tilstede.
2. Metoden for innsyn må være beskrevet før man setter i gang.
3. Innsynet skal dokumenteres, inklusive hvorfor innsynet ble foretatt, hvem som fattet beslutningen, hvem som var tilstede, metode for innsyn og resultatet.

Personopplysningsloven opphører ved dødsfall og arbeidsgiver kan gjennomgå vedkommendes e-post. Dette gjøres av sikkerhetsleder, IKT-sjef, arkivleder og personvernombud.

6.10 Ny behandling

Når nye behandlinger planlegges og før de iverksettes skal tabellen nedenfor fylles ut og gjennomgås med virksomhetsleder, sikkerhetsleder og personvernombud.

En protokoll over de personopplysningskategoriene som behandles i Melhus kommune foreligger hos sikkerhetsleder og på Intranett og EQS. Opplysningene omfatter:

Spørsmål	Besvarelse
1. Hva heter programmet som anvendes til behandling av personopplysningene?	
2. Hvor lenge har kommunen hatt programmet?	
3. Synspunkter på programmet	
4. Forhold til leverandør av programmet	
5. Planer og behov i tilknytning til program og bruk	
6. Kort om hvordan programmet brukes	
7. Hvor ligger program? I kommunen eller hos ekstern leverandør	
8. Hva slags personopplysninger behandles i programmet?	
9. Er personopplysningene sensitive, ref personopplysningslov?	
10. Mengde av personopplysninger – f eks antall individer, klienter	
11. Hvor lagres personopplysningene? Elektronisk og fysisk.	
12. Registreres og lagres personopplysninger i andre programmer og på andre lagringssteder? F eks Office og i filsystemet i mapper.	
13. Hvilken lovhjemmel ligger til grunn for behandling av personopplysningene?	
14.	
15. Hvem har ansvar for brukeradministrasjon av programmet?	
16. Hvilke brukere har tilgang til	

Spørsmål	Besvarelse
programmet	
17. Hvordan vurderer du kompetanse hos brukerne av programmet?	
18. Har brukerne fjernaksess til programmet?	
19. Utveksles personopplysningene elektronisk med andre instanser internt eller eksternt? Hvis ja, hvordan og med hvem? Er personopplysningene kryptert i forsendelsen?	
20. Brukes personopplysningene mobilt? Brukes bærbar PC? Minnepinne? Er personopplysningene kryptert når de er "på farten"?	
21. Andre sikkerhetsaspekter du vil nevne?	
22. Har det forekommet sikkerhetsbrudd, hendelser?	

7.0 Opplæring og kompetanse

Melhus kommune har en strategi for informasjonssikkerhet, hvor det er iverksatt tiltak for å ivareta Personopplysningslovens og Datatilsynets krav til personsikkerhet.

Melhus kommune har gjennomført en rekke tekniske tiltak som har løftet sikkerheten og stabiliteten på infrastruktur og driftsmiljø. Fokus fremover blir å videreføre tekniske sikkerhetstiltak som sørger for at rett person får tilgang til rett informasjon til rett tid.

Personopplysningsloven pålegger den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Dette omfatter å sørge for at tilstrekkelig sikkerhetsfaglig kompetanse er tilgjengelig hos den behandlingsansvarlige. I tillegg til ansvar for sikkerheten i egen organisasjon, må den behandlingsansvarlige også forsikre seg om at informasjonssikkerheten er tilfredsstillende hos kommunikasjonspartnere og leverandører.

Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av planlagte og systematiske tiltak..

Det er særlig to typer ansvar som det må skilles mellom når noen publiserer personopplysninger i sosiale medier. Det ene dreier seg om ansvaret for Melhus kommunes egne innlegg, mens det andre gjelder ansvaret for innhold som brukerne publiserer i Melhus kommunes kanaler.

Melhus kommune skal derfor:

- vektlegge kompetanse og utnyttelsesgrad ved anskaffelse, endringer og utvidelse av IKT-løsninger,
- gi opplæring, slik at ansatte og folkevalgte får nødvendig kompetanse til å ta i bruk og effektivt utnytte de respektive systemer.
- gjennomføres opplæring i informasjonssikkerhet på alle nivå
- årlig gjennomføre ledelsens gjennomgang
- gjennomføre KOMPIS-programmet i kommunen
- presentere heftet Ansatte og sikkerhetskultur i personalmøter
- legge ut Personvernerklæring på Melhus kommunes hjemmeside
- risikovurdere behandling av personopplysninger.

8.0 Databehandleravtale

Hvis hele eller deler av behandlingen av personopplysninger settes ut til andre virksomheter/ databehandler, skal forholdet mellom kommunen (*behandlingsansvarlig*) og databehandleren være regulert i en avtale – *databehandleravtale*. Dette reguleres av personopplysningsloven § 13, jf. § 15. Tilsvarende gjelder for helseregisterlovens § 16, jf. § 18.

En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av annet avtaleverk. En *databehandler* kan ikke behandle personopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Den behandlingsansvarlige skal forsikre seg om at databehandleren har tilstrekkelig sikkerhetsnivå, jf. personopplysningslovens § 15 (helseregisterlovens § 18).

Behandling av *sensitive personopplysninger* vil antagelig kreve en mer detaljert avtale enn en avtale om et enkeltstående faktureringsoppdrag.

For mer informasjon se: http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/

9. Kommunenes utlegging av dokumenter på Internett

Må forvaltningen ta personvernhensyn ved utlegging av dokumenter på internett?

Datatilsynet sendte i 2003 en forespørsel til Justisdepartementets lovavdeling om tolkning av personopplysningsloven i forhold til offentlighetsloven. Nå foreligger svaret fra lovavdelingen.

Personvernhensyn må tas
Lovavdelingen kom i sitt svar til at forvaltningens internett-publisering av dokumenter også omfattes av personopplysningsloven. Dette vil si at personvernhensyn må veies mot forhold som taler for publisering.

Bakgrunn for saken
Datatilsynet så at flere offentlige instanser begynte å legge ut alle inn- og utgående dokumenter på internett, bortsett fra dokumenter unntatt ved taushetsbestemmelser. Offentliggjøringen ble ikke vurdert i forhold til personopplysningsloven. Det ble dermed, etter Datatilsynet oppfatning, bare taushetsplikten i særlovene som regulerte hvorvidt opplysninger kunne publiseres eller ikke. Datatilsynet mente at dette ikke var i samsvar med intensjonene i personopplysningsloven, og ba om Justisdepartementets vurdering.

Personopplysningsloven skal ikke begrense innsynsretten etter offentlighetsloven. Men innsynsretten etter offentlighetsloven er knyttet opp mot en bestemt, avgrenset sak eller dokument: Den som ber om innsyn i en bestemt sak skal få det så sant ikke taushetsbestemmelsene som gjelder for saken, gjør at saken likevel ikke kan gis ut. Meroffentlighetsprinsippet sier i tillegg at

forvaltningen skal vurdere om dokumenter som kan unntas likevel kan utleveres, for eksempel ved å sladde enkelte opplysninger.

9.1 Bruk av video- og fotokamera

Dagligdagse gjøremål som filmes eller fotograferes for å studere samspillet mellom mennesker, regnes ikke som sensitive opplysninger. Denne bruken vil derfor verken være melde- eller konsesjonspliktig. Det bør heller ikke by på noe problem om for eksempel lærere tar bilder av elever for å henge opp i klasserommet eller for å gi til de foresatte.

Om man filmer eller fotograferer enkeltindivider for å eksempelvis studere atferdsvansker, vil det derimot kunne anses som sensitive opplysninger. Slik bruk krever samtykke fra de foresatte, og den vil være meldepliktig.

Ved bruk av digitalt kamera og lagring på PC må man være oppmerksom på at behandlingen som regel vil være konsesjonspliktig.

Slik dokumentasjon lagres derfor ikke på PC, men på minnebrikke (en brikke pr. behandling) som lagres i fysisk arkivmappe.

9.2 Personvern i skolen og barnehagen

Utgangspunktet er at fødselsnummer berre kan innhentast når ein har eit sakleg behov for ei sikker identifisering og dette er umogeleg å oppnå ved bruk av andre metodar.

- I dei fleste tilfella er det nok å bruke namn, adresse og fødselsdato for å sikre ei riktig identifisering, seier Christine Ask Ottesen, juridisk fyrstekonsulent i Datatilsynet. Ho understrekar at det ikkje er eit argument for bruk av fødselsnummer at systemet er tilrettelagt slik eller at det er praktisk i somme samanhengar.

Barn sitt fødselsnummer
Det vil vere enkelte tilfelle der faren for forveksling av barna er spesielt stor, og der fødselsnummer bør nyttast. Dette kan for eksempel gjelde ved kommunale samordna opptaksprosessar. Ulike rapporteringsplikter knytt til karakterar i grunnskulen vil også krevje større tryggleik når mange elevar blir handterte. Konsekvensane av ei forveksling vil i denne samanhengen kunne få særs uheldige konsekvensar. Dette gjer at bruk av fødselsnummer kan vere nødvendig for ei sikker identifisering av kvar enkelt elev.

Føresette sitt fødselsnummer
Når det gjeld bruk av fødselsnummer til dei føresette, vil utgangspunktet vere det same som for barna. Det vil seie at normalt vil andre måtar å identifisere dei føresette på vere tilfredsstillande, og at det derfor ikkje er sakleg behov for å bruke fødselsnummer.

I barnehagesamanheng vil det likevel finnast spesielle forhold som taler for bruk av fødselsnummer. For eksempel er det spesielt viktig med ei sikker identifisering for å kontrollere føresette sitt inntektsforhold i samband med søknad om redusert betaling. For offentleg eigde barnehagar vil bruk av fødselsnummer kunne vere nødvendig dersom dei føresette ønskjer automatisk frådrag i sjølvmeldinga. I samband med kontantstønadordninga vil innhenting av dei føresette sine fødselsnummer også vere tillate.

9.3 Klasselister, fødselsnummer og bilder

I forbindelse med barns opphold i barnehage og skole, melder det seg ofte spørsmål som gjelder barnas personopplysninger. Når kan opplysninger utleveres, og hvilke opplysninger er det greit å gi? Datatilsynet har utformet noen retningslinjer.

Klasselister og lister over barn i barnehageavdelinger o.l.
Man kan få utdelt lister over klasser man er eller tidligere har vært elev i uten samtykke fra hver enkelt elev eller dennes foresatte. Dette gjelder kun dersom opplysningene skal brukes til private

formål, og dersom de ikke skal videredistribueres. Om man er foresatt til en elev i en klasse har man også rett til å få utlevert klasseliste for denne elevens klasse. Det samme gjelder opplysninger om barn i samme barnehageavdeling.

NB! Fødselsnummer (alle 11 sifre) skal ikke gis ut på slike lister.

Klasselistene som deles ut i en klasse, eller til foresatte, kan inneholde:

- Elevenes og foresattes navn, adresse og telefonnummer

Klasselister som deles ut til tidligere elever (for eksempel i anledning av invitasjoner til jubileum) kan inneholde:

- Elevenes navn i tillegg til daværende adresse og telefonnummer

Klasselister for klassestyrere, skolestyret, skolelege, skoletannlege og klassekontakter kan inneholde:

- Elevens navn, adresse, telefonnummer og fødselsdato
- Foresattes navn, adresse og arbeidsadresse
- Klasseangivelse, klasserom og klassestyrers navn

Datatilsynet sa i utgangspunktet at lister over avgangselever i grunnskolen ikke kunne utleveres til private skoler. Fylkesmannen, bl.a. i Oslo, kom til et annet resultat. Datatilsynet har bedt Kunnskapsdepartementet ta stilling til spørsmålet.

Kan skolen kreve å få elevens og foresattes fødselsnummer?
Skolen må ha elevens fødselsnummer (11 siffer) i sitt register. Denne opplysningen trengs til entydig identifisering av elevene.

Skolen kan registrere foresattes fødselsnummer dersom skolen har saklig behov for dette i forbindelse med administrasjon av skolen. For eksempel kan dette være aktuelt i forbindelse med betaling for skolefritidsordningen. Dette er fordi utgiftene kan trekkes fra på skatten, og derfor innberettes til skattemyndighetene. Dersom fødselsnummer registreres kun fordi systemet er lagt opp slik, er ikke kriteriet om saklig behov oppfylt. Hvis den som ber om fødselsnummer ikke kan vise til en lovhjemmel, eller ikke har et saklig behov, kan man nekte å gi fra seg opplysningene.
Les mer om skolers og barnehagers bruk av fødselsnummer her

Kan barnehager og skoler filme og fotografere barna?
Det må presiseres at det her er snakk om håndholdt kamera. Regelmessig kameraovervåking med fastmontert kamera blir noe annet, og vil reguleres av personopplysningsloven. En slik type overvåking må også meldes til Datatilsynet.

Dagligdagse gjøremål som filmes eller fotograferes for å studere samspillet mellom barn og voksne, regnes ikke som sensitive opplysninger. Denne bruken vil derfor verken være melde- eller konsesjonspliktig. Det bør heller ikke by på noe problem om lærere tar bilder av elever for å henge opp i klasserommet eller for å gi til de foresatte.

Om man filmer eller fotograferer enkeltelever for å for eksempel studere atferdsvansker, vil det derimot kunne anses som sensitive opplysninger. Slik bruk krever samtykke fra de foresatte, og den vil være meldepliktig.

Ved bruk av digitalt kamera og lagring på PC må man være oppmerksom på at behandlingen som regel vil være konsesjonspliktig.

Kan skolen legge ut bilder av elevene på Internett?
Bilder av elever er likestilt med personopplysninger. Dersom man publiserer bilder på Internett krever dette samtykke fra den enkelte elev, eller fra elevens foresatte dersom eleven er under 15 år.

(Samtykke kreves forøvrig også for publisering av bilder av ansatte på Internett.)
Mer detaljerte retningslinjer om bilder på Internett kan leses her

Kan skolen loggføre og kontrollere elevenes internettbruk?
Hvis formålet med loggføringen er å kontrollere sikkerheten i datasystemet, trenger ikke skolen samtykke fra elever eller foresatte. Ved andre formål må skolen få samtykke fra den enkelte elev, eller fra foresatte om eleven er under 15 år. Skolen skal uansett informere elevene tydelig om at de legger igjen spor etter seg når de bruker maskinene. Det skal også opplyses om at sporene vil bli undersøkt, og hvorfor skolen gjør dette. Nye elektroniske læringsverktøy kan også gi vanskelige problemstillinger i forhold til personvern.

Er skolen ansvarlig for publisering av opplysninger om elevene i pressen?
Journalistisk virksomhet er unntatt store deler av personopplysningsloven. Ved intervju og fotografering er det eleven, og ikke skolen, som gir fra seg opplysninger. I slike tilfeller er det andre lover enn personopplysningsloven som gjelder. Pressens etiske komité og opplæringsloven kan blant annet være aktuelle her. Alle journalister må følge "Vær varsom plakaten", der det blant annet gis retningslinjer om intervju av barn.

Kan foresatte fotografere barna på skolen eller i barnehagen?

Ja, foresatte kan fotografere eller filme barna sine på arrangementer i skolen eller barnehagen, slik som adventsfest, luciafeiring, fremføringer osv. Skolen/barnehagen står imidlertid fritt til å lage egne retningslinjer som er tilpasset forholdene på det enkelte stedet. Det kan for eksempel være fotoforbud.

Men; hvis bildene/filmen skal publiseres på Internett og det er med andre barn på bildene/filmen, må man ha samtykke fra disse barnas foresatte først.

9.4. Lagring av sensitive personopplysninger i skole og barnehage

Skolene og barnehagene i Melhus har i 2014 ikke tilfredsstillende elektronisk lagringsmedium for sensitive personopplysninger. Det er i arkivplanen for Melhus kommune lagt retningslinjer for lagring av sensitive personopplysninger.

Sensitiv informasjon skal lagres i sikker sone. Sensitive opplysninger (IOP-er) kan inntil videre lagres elektronisk slik:
Opplysningene skrives ut på papir og lagres i elevmappen. I tillegg kan om ønsket informasjonen lagres på minnepenn som oppbevares i elevens mappe. Sensitiv informasjon må deretter slettes fra andre lagringsmedier som PC.

10.0 Avvikshåndtering

Sikkerhetsleder har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser ved brudd på konfidensialitet eller integritet samt enkeltpersoners brudd på sikkerhetsreglene. Hvis personopplysninger er kommet på avveie eller det er mistanke om det samme, skal Datatilsynet orienteres.

IT driftsansvarlig har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser relatert til tilgjengelighet, konfidensialitet eller integritet på IT-infrastruktur og tjenester.

Fagsystemansvarlig har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser relatert til tilgjengelighet, konfidensialitet eller integritet på egne systemer.

Dersom personopplysninger håndteres i strid med fastlagte rutiner eller ved mistanke om eller dokumentert brudd på informasjonssikkerhet, skal Melhus kommune iverksette

avviksbehandling.

Formålet med avviksbehandling er å bringe avviket til opphør, gjenopprette normal tilstand, og hindre gjentagelse. Dersom det ikke er samsvar mellom fastlagte rutiner og hvordan personopplysninger håndteres eller informasjonssystemet benyttes, skal resultatet fra avviksbehandling benyttes som grunnlag ved gjennomgang og endring av de aktuelle rutiner.

Eksempler på situasjoner som gjør det nødvendig å iverksette avviksbehandling:

- Ved utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering.
- Ved lagring av personopplysninger uten samtykke eller annet behandlingsgrunnlag.
- Når medarbeidere benytter informasjonssystemet uten autorisasjon.
- Ved feil i utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet.
- Henvendelse om innsyn har blitt avvist grunnet medarbeiderens manglende kjennskap til rutinene.

Avviksbehandling skal dokumenteres i henhold til alminnelige rutiner for avviksbehandling i EQS. Se nærmere om prosedyrer: http://mk-sv-eqs01/eqs/?pid=melhus&DocumentID=2649

11.0 Fysisk sikkerhet

Adgang til Melhus kommunes lokaler for eksternt (og internt) personell skal godkjennes av aktuell linjeleder og følge retningslinjer for tildeling av adgang. Adgang skal begrenses til det minimum av lokaler som vedkommende har behov for.

Adgangskontroll med bruk av adgangskort med personlig kode utenfor arbeidstid eller nøkkel, skal være montert.

Arkiv, datarom og rom med annet sentralt IT-utstyr skal sikres og plasseres slik at det er mulig å begrense adgangen til området. Dør til slike områder skal alltid være låst. Dette gjelder også rom med sensitive personopplysninger og opplysninger gradert etter andre lover.

Utrangerte harddisker beskyttes tilsvarende servere.

Ytterdører skal være låst etter arbeidstidens slutt.

Når kontor forlates skal kontordør låses.

Reserve besøkskort, adgangskort, nøkler og passord skal lagres i safe eller på annen sikker måte.

Alarmsystemer
Melhus kommunes adgangskontrollsystem skal gi alarm ved forsøk på uautorisert adgang til vaktselskap.

Melhus kommunes døgnkontinuerlig innbruddsovervåking skal gi automatisk alarm til egen vakt. Dette gjelder også for strømbrudd, brann og kjøling av datarom.

12.0 Ledelsens gjennomgang

Ledelsen i Melhus kommune skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av sikkerhet i tilknytning til informasjonssystemene. Ledelsen skal kontrollere at disse er i samsvar med Melhus kommunes behov og eventuelt oppdatere mål, strategi og organisering. Gjennomgangen gjennomføres i henhold til rutine beskrevet i ledelsens gjennomgang.

Ved ledelsens gjennomgang deltar representanter fra Melhus kommunes øverste ledelse sammen med sikkerhetsleder og IT-leder. Praktisk organisering av gjennomgangen, utarbeidelse av rapport og iverksetting av eventuelle tiltak er lagt til sikkerhetsleder.

I ledelsens gjennomgang av informasjonssystemet skal bl.a. følgende vurderes:

- Resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet.
- Endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder:
- Endringer i offentlige sikkerhetskrav.
- Endringer i de personopplysninger Melhus kommune skal behandle.
- Endringer i trusselbildet som bl.a. beskrevet i rapport fra utførte risikovurderinger.
- Om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet.
- Overordnet behandling av alvorlige avvik og hendelser.

Hensikten med ledelsens gjennomgang er:

- Følge opp de mål som er satt
- Gjøre korrigerende tiltak
- Vurdere oppfølging av korrigerende tiltak
- Endring av mål for prosess
- Sørge for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelige og effektive og at det tilfredsstiller relevante krav i personopplysningsloven og -forskriften.

Det er utarbeidet sikkerhetsmål for Melhus kommune. Sikkerhetsmålene gjennomgås og bakgrunnsmateriale for gjennomgangen vil være:

- Resultater og hovedkonklusjoner fra risikoanalyser og egenkontroll
- Endringer i offentlige sikkerhetskrav, som kan medføre vesentlig endringer for Melhus kommune
- Vurdere om tilstrekkelige ressurser er tilgjengelige for å ivareta internkontroll og informasjonssikkerhet

Det er ledelsen ved Melhus kommune som har ansvar for å gjennomføre ledelsens gjennomgang. Sikkerhetsleder har ansvar for å tilrettelegge gjennomgangen. Ledelsens gjennomgang gjøres normalt en gang pr. år.

Revisjon av de elementer som er styrende for internkontroll og informasjonssikkerhet, som:

- Internkontroll
  Vurdere endringer i omfang av dagens internkontroll
- Sikkerhetsmål og -strategi
  Vurdere eventuelle forslag til endringer i sikkerhetsmål og sikkerhetsstrategi, dersom endringene i vesentlig grad har økonomiske eller andre virksomhetsmessige konsekvenser
- Risiko- og sårbarhetsanalyse
  Ønske om ny funksjonalitet som medfører vesentlige investeringer eller endringer i eksisterende sikkerhetskonsept
- Virksomhetskritisk informasjon og/eller system
  Vurdering av endringer i hvilken informasjon eller hvilke systemer som er virksomhetskritisk for Melhus kommune

Ledelsen går detaljert gjennom de alvorligste hendelsene og avvikene som har vært gjennom året, kun summarisk gjennom de mindre alvorlige. Diskusjon bør omfatte årsaker til hendelser og avvik i vid forstand og hvordan hendelser og avvik er håndtert.

Forbedringstiltak, gjennomføring av tiltak til fastsatte tidspunkter, utarbeides av sikkerhetsleder på bakgrunn av oppsatte mål, innen områdene:

- Organisering av sikkerheten
- Partnere og leverandører
- Personell og sikkerhet
- Fysisk sikkerhet
- Systemteknisk sikkerhet
- Dokumentsikkerhet
- Beredskap

Forbedringstiltakene skal godkjennes av rådmannen.

Oppfølging av sikkerhetsmål for å se om de nås og om forbedringstiltak og korrigerende tiltak virker, gjøres blant annet gjennom egenkontroll. En plan for egenkontroll må derfor utarbeides.

Oppfølging av at forbedringstiltakene virker, gjøres i forbindelse med ledelsens gjennomgang, som gjennomføres normalt en gang pr. år.

Sikkerhetsleder skriver referat fra ledelsens gjennomgang og dette distribueres til ledelsen ved Melhus kommune. I referatet skal det tydelig fremgå de avgjørelser og aksjoner som er bestemt og med hvilken begrunnelse.

Eksempel på rapport fra ledelsens gjennomgang av informasjonssystemet og av informasjonssikkerheten er gjengitt nedenfor:

Rapport fra ledelsens gjennomgang 2006	Virksomhet: XX	Skrevet av: NN	Dato: 1.12.2006	Arkivref: xx.yyyy
Deltagere: Virksomhetsleder NN Sikkerhetsansvarlig NN IT-driftsleder NN				
Distribusjon: Møtedeltakerne				
Saknr.	Sak		Aksjon	Ansv./ frist
1/06	Rapporter fra utførte sikkerhetsrevisjoner. Rapportene fra sikkerhetsrevisjoner ble lagt fram uten merknader			
2/06	Behandling av registerte sikkerhetsbrudd og logger. Innbrudd på nettsted bør gi endret sikkerhetsstrategi		Det innhentes bistand til endring.	IT-driftsleder, 15.12.06
3/06	Behandling av foreslåtte nye løsninger. Prosjektforslaget for bruk av hjemmekontor ble godkjent.			

Resultatene dokumenteres i rapport i henhold til mal i dokumentet **Ledelsens gjennomgang.**

Vedlegg 1: Definisjoner

Emne	Definisjon
Autorisert tilgang	(Innen IKT) Godkjent og tildelt tilgang til et eller flere informasjonssystemer.
Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes
Behandling av helseopplysninger	Enhver formålsbestemt bruk av helseopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.
Databehandler	En juridisk enhet som behandler personopplysninger på vegne av den behandlingsansvarlige.
Forsettelig	Hendelsen skjer ved en bevisst handling hvor en har kunnskap om at det som gjøres kan forårsake et sikkerhetsbrudd.
Helseopplysninger	taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson.
Informasjonssikkerhet	Personopplysningsloven (§13) stiller krav om at virksomheten «*skal gjennom planlagte og systematiske tiltak sørge for at tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger*».
Informasjonssystemet	Samlebetegnelse på alt PC-utstyr, systemer og

	nettverkskomponenter som inngår i kommunens elektroniske databehandling.
Integritet	Å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige.
Internkontroll	Internkontroll er ledelsens verktøy for å styre aktivitet i virksomheten slik at driften skjer i overenstemmelse med lover og regler. Samtidig er styringssystemet medarbeidernes verktøy for å utføre oppgaver på en forsvarlig og sikker måte.
Kompromittering	Brudd på konfidensialitet, tilgjengelighet eller integritet.
Konfidensialitet	Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.
Overlegg	Systematisk eller planlagt aktivitet som kan medføre et sikkerhetsbrudd.
Personopplysninger	Opplysninger og vurderinger som kan knyttes til en enkeltperson.
Personopplysningsforskriften	Forskrift til personopplysningsloven, 15. desember 2000 nr. 1265.
Personopplysningsloven (POL)	Lov om behandling av personopplysninger, 14. april 2000 nr. 31.
Sikkerhetshendelse	En hendelse som får konsekvenser for informasjonssikkerheten i kommunen
Tilgjengelighet	Å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.
Uaktsomhet	Hendelsen skjer ved uhell, feil, tilfeldighet, ukyndighet eller tilsvarende som kan medføre et sikkerhetsbrudd.

Vedlegg 2: Sentrale lover, forskrifter og retningslinjer

For kommunens informasjonssikkerhet gjelder en rekke lover, forskrifter og bestemmelser som bl.a. tar sikte på å hindre at noen uten lovlig hjemmel får tilgang til person-/ klientopplysninger og andre opplysninger som er unntatt offentlighet. Alle berørte ledere og medarbeidere skal gjøres kjent med og følge det til enhver tid gjeldende lovverk.

Følgende lover og bestemmelser har relevans for så vel dokument- som databehandling i etaten:

Personopplysningsloven (POL) gjeldende fra 1.1.2001, omhandler bl.a. krav til melde- og konsesjonsplikt i forbindelse med behandling av personopplysninger. Meldinger og konsesjonssøknader fylles ut via www.datatilsynet.no

Forskrifter til POL, gjeldende fra 1.1.2001, omhandler bl.a. hvilke sikkerhetsløsninger som må iverksettes for at behandlingsansvarlig virksomhet skal ivareta kravet til konfidensialitet, integritet og tilgjengelighet ved behandlingen av personopplysninger

Lov om barnevernstjenester (Barnevernloven) av17. juli 1992. § 6-7. omhandler krav til taushetsplikt: **”**Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, en institusjon, et senter for foreldre og barn eller et omsorgssenter for mindreårige etter denne loven, har

taushetsplikt etter forvaltningsloven §§ 13 til 13 e. Overtredelse straffes etter straffeloven § 209. Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted. Opplysning om en klients oppholdssted kan likevel gis når det er klart at det ikke vil skade tilliten til barneverntjenesten, institusjonen eller senteret for foreldre og barn å gi slik opplysning. Opplysninger til andre forvaltningsorganer, jf. forvaltningsloven § 13 b nr. 5 og 6, kan bare gis når dette er nødvendig for å fremme barneverntjenestens, institusjonens, senteret for foreldre og barns eller omsorgssenteret for mindreåriges oppgaver, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse. Også yrkesutøvere i medhold av helsepersonelloven kan gis opplysninger etter denne bestemmelsen. Uten hinder av taushetsplikt skal barnevern tjenesten av eget tiltak gi opplysninger til helse- og omsorgstjenesten i kommunen når det er grunn til å tro at en gravid kvinne misbruker rusmidler på en slik måte at det er overveiende sannsynlig at barnet vil bli født med skade, jf. helse- og omsorgstjenesteloven § 10-3. Også etter pålegg fra de organer som er ansvarlige for gjennomføringen av helse- og omsorgstjenesteloven, plikter barneverntjenesten å gi slike opplysninger. Er et barn bortført fra barnevernet, skal barnevern-tjenesten gi opplysninger til myndighetene i barnets oppholdsstat, med mindre det ikke er forsvarlig eller til barnets beste. Dersom et barns interesser tilsier det, kan fylkesmannen eller departementet bestemme at opplysninger skal være undergitt taushetsplikt, selv om foreldrene har samtykket i at de gjøres kjent.»

Lov om sosiale tjenester m.v. (sosialtjenesteloven) av 18. desember 2009**.** § 45 omfatter opplysningsplikt til barneverntjenesten: Personell som arbeider innenfor rammen av denne loven skal i sitt arbeid være oppmerksom på forhold som kan føre til tiltak fra barnevernstjenestens side. Uten hinder av taushetsplikt skal personellet av eget tiltak gi opplysninger til barnevern- tjenesten, når det er grunn til å tro at et barn blir mishandlet i hjemmet eller det foreligger andre former for alvorlig omsorgssvikt, jf. lov om barneverntjenester §§ 4-10 til 4-12, eller når et barn har vist vedvarende alvorlige adferdsvansker, jf. samme lov § 4-24. Organene som er ansvarlige for gjennomføringen av lov om barneverntjenester, kan også pålegge personellet å gi slike opplysninger».

Lov om endringer i lov 17. juli 1992 nr. 100 om barneverntjenester og lov 13. desember 1991 nr. 81 om sosiale tjenester (sosialtjenesteloven) m.v.

Lov om familievernkontorer (familievernkontorloven) av 19. juni 1997. § 5 – 7 omhandler krav til taushetsplikt: «Enhver som utfører arbeid eller tjeneste for et familievernkontor har taushetsplikt etter helsepersonelloven §§ 21 og 23 med mindre noe annet fremgår av loven her. Overtredelse av taushetsplikt etter denne bestemmelsen kan straffes etter straffeloven § 209. Den som foretar mekling etter lov om ekteskap § 26 og barneloven § 51 og § 61 første ledd nr. 2 har taushetsplikt om det som kommer fram om personlige forhold i forbindelse med oppdraget. §§ 6, 7, 9 og 10 i loven her gjelder tilsvarende. Taushetsplikt er ikke til hinder for at opplysninger gjøres kjent for dem opplysningene direkte gjelder, eller for andre i den utstrekning de som har krav på taushet samtykker. For barn under 16 år, skal samtykke gis av foreldre eller foresatte. Etter hvert som barnet utvikles og modnes skal barnets foreldre høre hva barnet har å si før samtykke gis. Det skal legges vekt på hva barnet mener. Er barnet mellom 12 og 16 år, skal det legges stor vekt på hva barnet mener. Dersom et barns interesser tilsier det kan fylkesmannen eller departementet bestemme at opplysningene skal være undergitt taushetsplikt selv om det foreligger samtykke etter annet ledd. Taushetsplikt er ikke til hinder for at opplysninger gjøres kjent for annet personell ved det enkelte kontor av hensyn til klientbehandlingen med mindre klienten motsetter seg dette, og det etter forholdene kan og bør respekteres».

Lov om barnehager (barnehageloven) av 17. juni 2005
Lov om barneombud (barneombudsloven) av 6. mars 1981
Lov om folketrygd (folketrygdloven) av 28. februar 1997

Lov om adopsjon av 28.februar 1986

Forvaltningsloven av 10. februar 1967 inneholder bl.a. regler om taushetsplikt (§§13-13e), om informasjons- og veiledningsplikt, om varsling og innsyn og om klager og omgjøring av enkeltvedtak saksbehandlingsregler for forvaltningen, herunder regler om habilitet for saksbehandlere og andre som har med saken eller saksbehandleren å gjøre

eForvaltningsforskriften omhandler regler for elektronisk kommunikasjon i og med forvaltningen.

Offentleglova av 19. mai 2006 inneholder bestemmelser om i hvilken grad forvaltningens (etatens) saksdokumenter skal være tilgjengelige for offentligheten. Hovedregelen er at dokumentene er tilgjengelige, hvis ikke denne loven eller andre lover bestemmer noe annet. Offentlighetsloven har også en bestemmelse som sier at selv om forvaltningen kan hindre offentlig innsyn, skal det vurderes om dokumentene allikevel skal gjøres tilgjengelige hvis det kommer en forespørsel; dette kalles meroffentlighet

Forskrift om internkontroll - Helse, Miljø, Sikkerhet (HMS)

Lov om offentlige anskaffelser

Lov om arkiv av 4. desember1992 og tilhørende forskrifter

Lov om opphavsrett til åndsverk m.v.(**åndsverkloven**) av 12.5.1961, jfr. EUs direktiv om rettslig beskyttelse av edb-program

Straffeloven av 20. mai 2005 der bl.a. § 209 om bl.a. taushetsplikt for bl.a. offentlig ansatte

Lov om elektronisk (digital) signatur

Sikkerhetsloven av 20. mars 1998, omhandler opplysninger som er av betydning for rikets selvstendighet og sikkerhet, dvs skjermingsverdig informasjon. Loven gjelder for alle forvaltningsorgan.

Vedlegg 3:
Personvernerklæring Melhus kommune

Denne erklæringen redegjør for Melhus kommunes behandling av personopplysninger. Erklæringen er ment å gi informasjon til innbyggere og andre brukere av Melhus kommunes tjenester. Samtidig ønsker vi at erklæringen skal bidra til trygghet og tillit i forhold til at personopplysninger blir behandlet korrekt og sikkert i Melhus kommune.

Informasjonssikkerhet

Etter personopplysningsloven har vi ansvar for å sørge for at alle personopplysningene om deg er tilstrekkelig sikret. Vi har innført rutiner som skal gi nødvendig sikkerhet. Melhus kommune har et eget internkontrollsystem som følger opp dette.
Vi sikrer at kun de som har et tjenstlig behov får tilgang til opplysningene om deg. Videre sikrer vi at opplysninger ikke kan endres eller slettes av andre enn de som er autorisert til å gjøre dette. Vi sikrer at personopplysningene er tilgjengelige når det er nødvendig for å utføre våre arbeids-oppgaver, for å gi deg en best mulig tjeneste. Vi revurderer våre rutiner periodisk slik at sikkerheten til enhver tid skal være så god som mulig. Dersom vi oppdager at en rutine ikke fungerer etter hensikten, følges dette grundig opp.

Personvern og taushetsplikt

Ansatte i Melhus kommune plikter å hindre at andre får adgang eller kjennskap til personlige opplysninger om deg. Dette gjelder også andre opplysninger som skal hemmeligholdes av hensyn til ditt personvern. I enkelte saker er taushetsplikten særlig streng.

Personvernombud

Melhus kommune har eget personvernombud som skal påse at kommunen behandler personopplysninger etter bestemmelser i personopplysningsloven og personopplysningsforskriften.

Du har rett til innsyn

Du kan henvende deg til en hvilken som helst av våre avdelinger og be om å få vite hva slags personopplysninger vi har om deg, hva de skal brukes til, og hvor de er innhentet fra. Dette gjelder både elektroniske og manuelle registre. Du skal få svar innen 30 dager.

Personopplysninger skal slettes når behovet for behandlingen faller bort og sletting kan foretas i medhold av arkivlovgivningen. Du har rett til å klage til Datatilsynet dersom du mener behandlingen er i strid med reglene.

Du kan kreve at feil blir rettet

I utgangspunktet skal vi av eget tiltak rette mangelfulle eller feilaktige opplysninger. Men oppdager du selv at noe er feil – gi beskjed til oss, så retter vi dette umiddelbart.

Du kan kreve at unødvendige opplysninger om deg blir sperret eller slettet Vi sletter eller sperrer opplysninger som ikke lenger er nødvendige for formålet med registreringen. Dette gjelder ikke dersom opplysningene skal oppbevares i henhold til annen lovgivning, for eksempel regnskapsloven og arkivloven.

Du skal kunne utøve dine rettigheter gratis

Når du ber om innsyn, retting og sletting er dette gratis.

Melhus kommunes internettsider

Melhus kommune innhenter vanlig besøksstatistikk for sine nettsider. Opplysningene benyttes kun i forbindelse med drift og videreutvikling av Melhus kommunes nettsider.

E-post og skjema på internett

Det er sikkerhetsmessige svakheter ved bruk av e-post. Melhus kommune har derfor innført automatiske rutiner for viruskontroll av e-post. Det betyr at din e-post vil kunne bli stoppet automatisk. Dersom du ikke mottar svar på din e-posthenvendelse innen rimelig tid, ta kontakt for eksempel på telefon. Kontaktinfo finner du på vår webside: www.melhus.kommune.no.

Vår e-postadresse postmottak@melhus.kommune.no kan benyttes til enkle spørsmål og henvendelser.

Vær oppmerksom på at bruk av e-post og åpne skjema på internett har svakheter som gjør at opplysninger kan komme på avveie. Send derfor ikke sensitive eller fortrolige opplysninger med e-post eller via internettskjema.

Partsinnsyn etter forvaltningsloven

Dersom du henvender deg til oss med en klage, vil Melhus kommune normalt vise til, eller legge ved, din henvendelse når Melhus kommune tar kontakt med den innklagede parten. Du kan be om at Melhus kommune ikke oppgir hvem du er ved henvendelser til den andre parten. Det skal imidlertid

svært mye til å nekte en part innsyn i saken dersom han ber om det. Melhus kommune kan derfor ikke garantere anonymitet ved slike henvendelser.

Pressens og allmennhetens innsyn etter offentlighetsloven

Hovedregelen etter offentlighetsloven er at forvaltningsorganers saksdokumenter er offentlig tilgjengelige. Det betyr at alle som spør om det, presse og andre, vil kunne gjøre seg kjent med innholdet i kommunens saksdokumenter. Din henvendelse til Melhus kommune vil dermed også være offentlig, enten den kommer i form av brev, telefaks eller e-post.
Melhus kommune håndterer imidlertid en del dokumenter som inneholder taushetsbelagte opplysninger. Slike dokumenter blir unntatt fra offentligheten. Interne dokumenter kan også unntas offentligheten.

Oversikt over personopplysninger

Melhus kommune har oversikt over alle fagsystem som inneholder personopplysninger. Alle slike løsninger er meldt inn og/eller søkt konsesjon for hos Datatilsynet, i det såkalte ”Meldesystemet”. Se www.datatilsynet.no. Meldesystemet sørger for en åpenhet rundt behandlingen av person-opplysninger i virksomheter. Systemet gjør det mulig for deg som enkeltperson å sjekke hvordan dine personopplysninger blir behandlet, slik at du kan ivareta dine rettigheter.

Videreformidling

Vi skal ikke selge, bytte eller på annen måte videreformidle informasjon av noen art om deg til tredjepart uten at du har samtykket til dette.

Spørsmål om personvern?

Dersom du har spørsmål om behandling av personopplysninger ber vi deg ta kontakt med oss. Se våre websider for kontaktinformasjon: www.melhus.kommune.no”

Vedlegg 4: Autorisasjon for tilgang til datasystemer - Taushetserklæring

Tilgang til datasystemer for eksterne konsulenter (leverandører)

Nedenstående konsulent/arbeider er med signatur på denne erklæring autorisert for tilgang til Melhus kommune's datasystemer, dog gjeldende for de systemer det er gitt oppdrag/vedlikehold på.

Autorisasjonen gjelder for:

☐ Tilgang til datasystemer via lokal pålogging eller sikret fjernaksess
☐ Fysisk tilgang til serverrom

Autorisasjonen gjelder kun i følge med autorisert IKT-konsulent eller IKT-leder, og har en varighet på to år fra signert erklæring.

Taushetserklæring

Jeg forstår at jeg i mitt arbeide vil kunne komme over opplysninger som ikke uvedkommende skal ha kjennskap til. Jeg forstår også at dette er regulert gjennom lover og regler.

Jeg forplikter meg til å utvise absolutt taushet overfor uvedkommende om forhold som jeg får kjennskap til ved mitt arbeide hos dem. Dette gjelder også overfor andre medarbeidere som tilhører virksomheten jeg jobber for. Dette gjelder spesielt anliggende som er regulert ved lov.

- Personopplysningsloven
- Forvaltningsloven § 13
- Straffeloven § 121 og § 144 og § 294
- Helsepersonelloven § 21 og § 67
- Markedsføringsloven § 7

Jeg er klar over
at brudd på taushetsplikten vil få alvorlige og strafferettslige følger, og at begrensningene også gjelder etter at jeg har ferdigstilt arbeide hos dere, eller sluttet hos nåværende arbeidsgiver.

Jeg erkjenner herved at jeg er kjent med Forvaltningslovens § 13 (Taushetsplikt), samt evt. gjeldende særlov, og er vitende om at overtredelse av gjeldende bestemmelser kan medføre straffeansvar etter Straffelovens § 121.

Firma: _____Sted/dato: _____

Navn (blokkbokstaver):_____

Underskrift: _____

Autorisert av: _____ Init.:_____

Vedlegg 5:Konsesjons- eller meldeplikt for personopplysningene?