Fra: Roar Dønheim <Roar.Donheim@melhus.kommune.no <mailto:Roar.Donheim@melhus.kommune.no>>
Sendt: fredag 8. mai 2020 12:30
Til: post@konsek.no <mailto:post@konsek.no>
Kopi: Katrine Lereggen <Katrine.Lereggen@melhus.kommune.no <mailto:Katrine.Lereggen@melhus.kommune.no>>; Geir Wormdal <Geir.Wormdal@melhus.kommune.no <mailto:Geir.Wormdal@melhus.kommune.no>>; Egil Johannes Hauge <egil.johannes.hauge@melhus.kommune.no <mailto:egil.johannes.hauge@melhus.kommune.no>>
Emne: Orientering til kontrollutvalget - personvern

Kontrollutvalget fattet i møte 13.2.2020 bl.a. følgende vedtak:
«Kontrollutvalget ønsker en orientering om Melhus kommune sine rutiner og prosedyrer når det gjelder personvern (GDPR). Skriftlig orientering sendes kontrollutvalgets sekretariat innen 8. mai 2020. Muntlig orientering gis på kontrollutvalgets møte 28. mai 2020.»

Ny lov om behandling av personopplysninger ble iverksatt 20.7.2018. Sentralt i den nye loven ligger forordning fra EU (2016/679) - personvernforordningen. Den legger premissene for den nye loven og gjelder for alle stater tilsluttet EU og EØS. Personopplysningsloven har implementert personvernforordningen i sin helhet med noen tilpasninger og lovteksten viser i meget stor grad til forordningen.

Personopplysningsloven stiller en rekke krav til behandlingsansvarlig (rådmannen) ved behandling av personopplysninger. Kort kan nevnes:

Godt personvern sikrer at behandling av personopplysninger skjer innenfor fastsatte krav om:
- *Tilgjengelighet* (for rett person, til rett tid, i rett form og på rett sted)
- *Integritet* (at informasjonen er korrekt og ikke forfalsket eller ødelagt eller feilaktig)
- *Konfidensialitet* (at informasjonen sikres mot uvedkommende innsyn, herunder utilsiktet utlevering)
- *Robusthet* (*at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser)*

*Reglene for behandling av personopplysninger bygger på noen grunnleggende prinsipper (**personvernprinsippene**). Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene:*
- *Lovlig, rettferdig og gjennomsiktig*
- *Formålsbegrensning*
- *Dataminimering*
- *Riktighet*
- *Lagringsbegrensning*
- *Integritet og konfidensialitet*
- *Ansvarlighet*

*Alle virksomheter har plikt til å legge til rette for at brukere/kunder får oppfylt rettighetene (**de registrertes rettigheter**) 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*

For å ivareta sikker og god behandling av personopplysninger har Melhus kommune utarbeidet rutiner og prosedyrer som omfatter bl.a.:

- Styrende dokument
- Ansatte og sikkerhetskultur
- Personvernerklæring, de registrertes rettigheter settes i fokus.
- Protokoll over behandlingsaktiviteter
- Oversikt over behandlingsaktiviteter
- Databehandleravtale
- ROS
- Personvernombud
- Avvikssystem
- Opplæring
- Omtale av hver enkelt kommer nedenfor.

For å ivareta krav om en systematisk tilnærming skal virksomhetene opprette system for internkontroll. Denne består gjerne av tre hovedelementer:

Styrende elementer, som i hovedsak retter seg mot ledelsen, herunder hvilke beslutninger og føringer de legger for internkontroll.

Gjennomførende elementer, som i hovedsak retter seg mot ansatte. Her finner man beskrivelse av rutiner som er tilpasset den enkeltes arbeidssituasjon.

Kontrollerende elementer, som bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.
Internkontroll kalles i ulike sammenhenger et kvalitetssystem, styringssystem eller ledelsessystem for etterlevelse av regelverk.

Styrende dokument

Datatilsynet skriver i sin veiledning:
«Styrende dokumentasjon gir en systembeskrivelse som inneholder policy og målsetning, identifiserte krav og plikter, intern organisering, ansvar og myndighet. Styrende dokumentasjon er overordnet i sin form og er spesielt ledelsesorientert.

Styrende dokumentasjon bør inneholde:

- virksomhetens mål og retningslinjer for vern av personopplysninger. Se spesielt personvernforordningen artikkel 1.
- identifisering av at tiltenkt lagring og behandling av personopplysninger samsvarer med lovens grunnkrav, se artikkel 5 og 6 i personvernforordningen. Det legges spesielt vekt på saklig behov og konkret definering av formål, herunder at opplysningene som lagres samsvarer med formålet.
- identifisering av hvilke generelle forpliktelser som er relevant for virksomheten, se artikkel 24-43 i

personvernforordningen
- organisering av virksomheten der intern delegering av ansvar og myndighet skal være entydig definert, se spesielt artikkel 24, 26, 28, 32, 37-39.
- beskrivelse av hvordan virksomheten ivaretar informasjonssikkerheten. Se artikkel 32-34.
- beskrivelse av hvordan ledelsen vil sørge for at virksomhetens aktiviteter er i samsvar med kravene i regelverket. En slik beskrivelse vil normalt ende opp i behov for gjennomførende dokumentasjon og kontrollerende dokumentasjon.»

Melhus kommune har i lengre tid hatt styrende dokumentasjon som er formulert i dokumentet Policy, regelverk rutiner og prosedyrer. Dette dokumentet er under en større revisjon for å tilpasses nytt lovverk og gi bedre veiledning til kommunens ledere, jf. Vedlegg. Forventes ferdigstilt i løpet av Mai måned.

Dokumentet beskriver de tre hovedelementene, styrende, gjennomførende og kontrollerende.

Ansatte og sikkerhetskultur

Dokumentet ansatte og sikkerhetskultur, jf vedlegg, er et opplæringsdokument for alle ansatte i Melhus kommune. Dokumentet er tilgjengelig på kommunens kvalitetssystem EQS. Dokumentet har implementeringsstøtte, dvs. at ansatte må kvittere ut at de har lest og forstått dokumentet. Ansatte og sikkerhetskultur er også under revisjon for å ivareta endringene som skjer i forbindelse med prosjektet *Smartere Melhus* med blant annet ny velferdsteknologo innføring av Microsoft 365 og Teams.

Personvernerklæring

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

Melhus er kommune har utarbeidet Personvernerklæring som gir veiledning til brukere/kunder (de registrerte) om sine rettigheter og veiledning til disse. Personvernerklæringen er lagt ut på kommunens hjemmeside lenke ligger nederst på framsiden:

<https://www.melhus.kommune.no/personvernerklaering.5740350.html>

Protokoll over behandlingsaktiviteter

Personvernforordningen (art. 30) pålegger alle virksomheter som behandler personopplysninger å føre protokoll over behandlingsaktiviteter som utføres under deres ansvar.

For å sikre god internkontroll skal behandlingsansvarlig ha oversikt over hvilke behandlinger og hvilke personopplysninger som behandles. Disse skal inngå i Protokoll over behandlingsaktiviteter. Personvernforordningen fastsetter hvilken informasjon protokollen skal inneholde. Det vises til vedlagte protokoll. Protokollen skal være skriftlig, elektronisk og på anmodning være tilgjengelig for tilsynsmyndigheten. Protokollen er tilgjengelig i kommunens kvalitetssystem EQS.

Oversikt over behandlingsaktiviteter

Det skal føres en sumarisk oversikt over behandlingsaktivitetene. Dette skal være en oversikt over protokollene og skal være tilgjengelig på kvalitetssystemet EQS.

Databehandleravtale

En databehandler er en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige (personvernforod. Art.4)

Melhus kommune har i dag databehandleravtaler med en rekke eksterne leverandører. Dette er leverandører som lever programvare hvor personopplysningen blir lagret hos leverandør, altså utenfor våre servere på Melhus rådhus. Disse må inngå avtale at de kun behandler personopplysningene etter våre retningslinjer. Dette for å unngå misbruk som bl.a. sal av opplysninger. Databehandleravtalene er tilgjengelig på kommunens kvalitetssystem EQS.

ROS/DPIA

Virksomheten skal gjennomføre en risikovurdering før personopplysninger behandles og før man tar i bruk et informasjonssystem. Virksomheten skal også gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i behandlinger, endringer av informasjonssystem eller endringer i trusselbildet.
En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas.
Melhus kommune gjennomfører risikoanalyser (ROS) av informasjonssikkerhet ved bruk av risikomodulen i kommunes krisehåndteringssystem CIM. Kommunen har utarbeidet egne kriterier for vurdering av konsekvenser, jf. eget vedlegg. Der er vedriene: Liv og helse, Konfidensialitet, Integritet, Tilgjengelighet og Omdømme lagt til grunn. Disse er verdsatt i en matrise.

Personvernombud

Et personvernombud skal gi råd om hvordan den behandlingsansvarlige best mulig kan ivareta personverninteressene. Offentlig virksomhet har plikt til å ha ombud. Foruten å gi råd til behandlingsansvarlig, skal ombudet bistå de registrerte og være kommunens kontaktpunkt til Datatilsynet.
Melhus kommune har opprettet eget personvernombud som også innehar rollen som rådgiver for rådmannen (behandlingsansvarlig).

Avvikssystem

Melhus kommune har utarbeidet egen avviksmodul for å behandle avvik. Avvikssystemet er en del av kommunens ordinære avvikssystem, men er tilpasset kravene om avviksmelding til Datatilsynet. Alle avvik som skyldes brudd på datasikkerheten skal meldes til Datatilsynet. Unntak fra dette gjelder hvis det er usannsynlig at avviket medfører en risiko for enkeltpersoners rettigheter eller personvern. Meldingsfrist til Datatilsynet er senest 72 timer etter at avvik ble oppdaget. Det er derfor innført en rutine om at alle avvik om brudd på datasikkerheten skal meldes til personvernombud/rådgiver. Er denne ikke tilgjengelig overføres meldingen automatisk til rådmannen etter 24 timer.

Opplæring

Opplæring av ansatte i informasjonssikkerhet i Melhus kommune skjer i hovedsak på disse områdene:

- **Heftet Ansatte og sikkerhetskultur er tilgjengelig på kommunens kvalitetssystem. Det forutsettes at alle ansatte har gjennomgått materialet og kvittert ut at det er lest og forstått**
- **Ved personalmøte i enhetene**
- **I samband med opplæring av ansatte innen Helse og omsorg**
- **Egne opplæringsvideoer (planlegges gjennomført i løpet av mai måned.**

Håper denne skriftlige orienteringen gir en grei oversikt over de rutiner og prosedyrer som gjelder for arbeidet med personvern. Ser fram til å gi en nærmere orientering på kontrollutvalgets møte 28.mai 2020.05.08

Mvh

MELHUS KOMMUNE
Plan
Roar Dønheim
rådgiver/personvernombud

Mobil 90832614
www.melhus.kommune.no <https://www.melhus.kommune.no/>